TAMPEREEN YLIOPISTO
Johtamiskorkeakoulu

RISKIENHALLINTAJÄRJESTELMÄN KEHITTÄMINEN SISÄISEN TARKASTUKSEN NÄKÖKULMASTA
Case: Pirkanmaan Osuuskauppa

Yrityksen taloustiede, laskentatoimi
Pro gradu -tutkielma
Toukokuu 2013
Ohjaaja: Petri Vehmanen

Anne Helander

TIIVISTELMÄ

Tampereen yliopisto	Johtamiskorkeakoulu; yrityksen taloustiede, laskentatoimi
Tekijä:	HELANDER, ANNE
Tutkielman nimi:	Riskienhallintajärjestelmän kehittäminen sisäisen tarkastuksen näkökulmasta Case: Pirkanmaan Osuuskauppa
Pro gradu -tutkielma:	76 sivua, 4 liitesivua
Aika:	Toukokuu 2013
Avainsanat:	riskienhallinta, sisäinen tarkastus, järjestelmän kehittäminen, riskienhallinnan arviointi

---

Riskienhallinnasta on tullut yhä keskeisempi osa organisaatioiden toimintaa. Tämä johtuu ennen kaikkea ympäristön nopeista muutoksista, muutosten ennustamisen vaikeudesta sekä 2000-luvun talouskriisistä. Riskienhallinnalla pyritään kuitenkin nykyään vahinkojen välttämisen ohella myös liiketoiminnallisen lisäarvon tuottamiseen. Riskienhallinnalta vaaditaankin yhä enemmän, joten riskienhallintaa ei voidakaan enää ajatella toteutettavan muusta toiminnasta irrallisena palasena. Vaatimusten täyttäminen edellyttää riskienhallinnan integroimista osaksi organisaation suunnittelua, päätöksentekoa ja johtamista.

Tämän tutkimuksen tavoitteena oli kehittää Pirkanmaan Osuuskaupan riskienhallintajärjestelmää varten suunnitelma, jonka avulla riskienhallinnasta saadaan rakennettua toimivampi ja tehokkaampi kokonaisuus. Tutkimus on luonteeltaan konstruktiivinen tapaustutkimus, jonka empiirinen aineisto kerättiin haastatteluin kohdeyrityksessä. Teoreettinen viitekehys rakennettiin sisäisen tarkastuksen riskienhallinnan arviointikriteerien ja niiden pohjalta muotoillun riskienhallintajärjestelmämallin ympärille. Aineiston kerääminen sekä sen analysointi toteutettiin teoreettisen viitekehyksen pohjalta. Aineistoa analysoimalla havaittiin yrityksen riskienhallintajärjestelmän nykytila, siihen liittyvät ongelmat sekä kehityskohteet. Tunnistetut kehityskohteet jaettiin neljään osa-alueeseen: riskienhallintaprosessi, ohjeistus, tasapainotettu mittaristo ja viestintä.

Tutkimuksen tavoitteen täyttämisen lisäksi tutkimuksessa vastattiin tutkimuksen tutkimusongelmaan: *Millainen on tehokas riskienhallintajärjestelmä sisäisen tarkastuksen näkökulmasta?* Tutkimusongelmaan vastattiin sekä sisäisen tarkastuksen riskienhallinnan kriteereitä listaamalla että teoreettisen riskienhallintajärjestelmän mallintamisella. Tutkimus täydentääkin aiempaa kirjallisuutta yhdistämällä sisäisen tarkastuksen riskienhallinnan arvioinnin kriteerit riskienhallintajärjestelmän kehittämistä käsittelevään tutkimukseen.

SISÄLLYS

1 JOHDANTO

1.1 Riskienhallinnan maailma

Tieto- ja viestintäteknologian nopea kehitys, globalisaatio, väestön rakenteessa tapahtuvat muutokset, muuttuvat markkinat, kilpailu ja lainsäädäntö asettavat suuria haasteita toimijoille, jotka pyrkivät hallitsemaan ja ennakoimaan tulevaa kehitystä seuraavien 10–20 vuoden aikana. Riskienhallinnan näkökulmasta tämä tarkoittaa, että sen painopisteen on pakko siirtyä perinteisestä teknisestä riskienhallinnasta kohti kompleksisuuden, epävarmuuden ja monimerkityksisyyden hallintaa, toisin sanoen kohti kokonaisvaltaisempaa riskienhallintaa. (Branson 2010, 51; COSO 2004, 13; Kimbrough & Componation 2009, 18; Räikkönen & Rouhiainen 2003, 3; Shenkir & Walker 2011, 4)

Riskienhallinnan luonne onkin muuttunut viimeisen vuosikymmenen aikana huomattavasti. Riskienhallinta ei ole enää vain vahinkoriskeiltä suojautumista, vaan sillä pyritään saavuttamaan myös todellisia liiketoiminnallisia hyötyjä. (Blumme, Karhu, Kontula, Laitakari, Linna, Nordin, Sovasto, Tarvainen, Tikkanen, Turakainen, Urrila & Vesa 2005, 79; The Economist Intelligence Unit 2007, 11) Yritystoiminnan riskejä pyritään tarkastelemaan yhtenä kokonaisuutena, jolloin myös riskien kytkentöjä toisiinsa voidaan paremmin ymmärtää. Lisäksi riskien tarkastelu osana organisaation strategista suunnittelua ja päätöksentekoa nähdään oleellisena tehokkaan riskienhallinnan kannalta. (Kaplan & Norton 2004, 27; Kupi, Keränen & Lanne 2009, 12)

Talouskriisi, joka alkoi vuonna 2007 yhdysvaltalaisista rahoituslaitoksista, osoittikin konkreettisesti, kuinka tärkeää riskien tehokas tunnistaminen ja hallinta on. Kriisi aiheutti paniikin, joka levisi globaaleille markkinoille ja käytännöllisesti katsoen jäädytti luottomarkkinat vuonna 2008. (McShane, Nair & Rustambekov 2011, 641) Kriisin syyllisiä ja siihen johtaneita syitä on pyritty selvittämään; riskienhallinnan toimimattomuutta on esitetty yhdeksi kriisin syistä (Fraser & Simkins 2010, 27).

Monimutkainen, epävarma ympäristö ja riskienhallinnan korostunut merkitys ovat johtanut siihen, että myös organisaation ulkopuoliset sidosryhmät ovat yhä kiinnostuneempia organisaatioiden riskienhallinnan tilasta ja vaativatkin yhä läpinäkyvämpää ja tehokkaampaa riskienhallintaa (PwC 2008, 3; The Economist Intelligence Unit 2007, 2, 6–7). Sisäisellä tarkastuksella on merkittävä rooli organisaation riskienhallinnan hyvyyden varmistamisessa. Sisäinen tarkastus arvioi riskienhallinnan tehokkuutta ja edistää näin toiminnallaan riskienhallinnan jatkuvaa parantamista. (Jorgensen 2011, 63; Lindow & Race 2002, 28; McShane, Nair & Rustambekov 2011, 641) Sisäisen tarkastuksen avulla voidaan varmistua siitä, että organisaatiossa ymmärretään sen riskit ja, että riskienhallinnan toimenpiteillä vastataan riskeihin tehokkaalla ja tarkoituksenmukaisella tavalla (Pickett 2005, 3).

Riskienhallintaan liittyvää kirjallisuutta on saatavilla runsaasti. Sisäisen tarkastuksen roolin muutos operatiivisesta toimijasta strategisella tasolla toimivaksi vaikuttajaksi on myös lisännyt huomattavasti kirjallisuutta sisäisen tarkastuksen puolella, erityisesti sen roolista ja tehtäväkentästä. Sisäisen tarkastuksen ammattiohjeistuksista on löydettävissä listauksia siitä, millaista riskienhallinnan tulisi olla sisäisen tarkastuksen näkökulmasta. Tutkimuksia, joissa yhdistettäisiin sisäisen tarkastuksen edellyttämät riskienhallinnan ominaisuudet ja riskienhallinta ei sen sijaan juurikaan ole. Tutkimuksen puute saattaa johtua siitä, että sisäisen tarkastuksen kriteerien mukainen riskienhallinta noudattelee hyvin pitkälle kokonaisvaltaisen riskienhallinnan yleisiä viitekehyksiä, mikä näkyy myös tässä tutkimuksessa arvioinnin lähdekirjallisuudessa. Tämä tutkimus tuo lisäarvoa aiempaan kirjallisuuteen yhdistämällä sisäisen tarkastuksen arviointikriteerit riskienhallintajärjestelmän kehittämistä käsittelevään tutkimukseen.

Kirjallisuudessa on keskitytty riskienhallinnan muodollisiin viitekehyksiin ja prosesseihin. Vaikka riskienhallintaprosessin olemassaolo on tehokkaan riskienhallinnan edellytys, paneudutaan tässä tutkimuksessa myös muihin tehokkuuden kannalta tärkeisiin tekijöihin: suotuisa organisaatiokulttuuri, ohjeistus ja tiedottaminen, roolijako, riskienhallinnan integrointi suunnittelu- ja päätöksentekoprosesseihin sekä jatkuva parantaminen. Lisäksi tutkimuksen case syventää aiempaa kirjallisuutta ja tarjoaa esimerkin siitä, mitä asioita yrityksen tulisi huomioida riskienhallintajärjestelmän kehittämisessä riskienhallinnan tehokkuuden ja toimivuuden parantamiseksi.

1.2 Tutkimuksen tavoite ja rajaukset

Tutkimuksen tavoitteena oli kehittää case-yrityksen riskienhallintajärjestelmää varten suunnitelma, jolla riskienhallinnasta voidaan rakentaa toimivampi ja tehokkaampi kokonaisuus. Tutkimusongelma on: *Millainen on tehokas riskienhallintajärjestelmä sisäisen tarkastuksen näkökulmasta?*

Riskienhallinnan arviointi kuuluu sisäisen tarkastuksen tehtäväkenttään. Sisäisen tarkastuksen arviointityöhön on olemassa ohjeistuksia ja standardeja, joiden pohjalta tutkimuksessa listataankin riskienhallinnan arviointikriteereitä. Tutkimuksessa muotoillaan sitten yleinen riskienhallintajärjestelmän malli, joka on sisäisen tarkastuksen kriteerien mukainen. Tutkimuksen empiirisessä osuudessa case-yrityksen riskienhallinnan nykytilan, siihen liittyvien ongelmien ja kehityskohteiden analysoinnin sekä teoreettisen riskienhallintamallin pohjalta muotoillaan kohdeyritykselle suunnitelma kohdeyritykselle sopivasta riskienhallintajärjestelmästä. Tavoitteiden saavuttamiseksi tutkimuksessa tutustutaan aiempaan riskienhallinnan ja sisäisen tarkastuksen kirjallisuuteen sekä case-yrityksen nykyiseen riskienhallintajärjestelmään haastatteluiden ja yritykseltä saatavan kirjallisen materiaalin avulla.

Tutkimuksessa vastataan tutkimusongelmaan tehokkaasta riskienhallintajärjestelmästä sisäisen tarkastuksen arviointikriteereitä listaamalla sekä niiden pohjalta mallinnetulla riskienhallintajärjestelmällä.

Riskienhallinnan kenttä on hyvin laaja ja siksi onkin tarpeellista tehdä joitakin rajauksia tutkimuksessa käsiteltävistä aihealueista. Tavoiteltaessa tehokkaampaa ja toimivampaa riskienhallintaa pitää yrityksellä olla käsitys toimintaansa liittyvien riskien kokonaisuudesta sekä niiden kartoittamiseen soveltuvista käytännöistä. Tässä tutkimuksessa yksitäisten riskien ja riskienhallintakeinojen syvempi tarkastelu rajataan kuitenkin tutkimuksen ulkopuolelle. Kohdeyrityksen osalta tehdään lisäksi rajaus, joka koskee sen riskienhallintaa eri organisaatiotasoilla. Tutkimus keskittyy pääosin vain strategisen ja taktisen tason riskienhallintaan. Rajaus on oleellinen siitä syystä, että yrityksen operatiivisen riskienhallinnan nykytila poikkeaa huomattavasti ylemmän tason riskienhallinnan tilasta. Operatiivisen taso riskienhallinta onkin huomattavasti paremmin organisoitu,

eikä näin ollen vaadi tällä hetkellä muutoksia. Kuitenkin tutkimuksen aineiston analysoinnin yhteydessä myös operatiivisen tason riskienhallinnan tilaa eritellään kokonaiskuvan hahmottamiseksi.

Sisäisen tarkastuksen arviointikriteereiden lähteistä tutkimukseen on valittu ne, jotka ovat yleisluonteisia ja näin soveltuvat moneen organisaatioon. Tutkimuksessa käytettyjä arvioinnin lähteitä on käsitelty kappaleessa 3.1. Tutkimuksen ulkopuolelle on jätetty muun muassa Cobit ja ISO 17799, jotka koskevat hyvää IT-hallintotapaa ja tietoturvallisuuden hallitsemista.[1] Näitä ei käsitellä tutkimuksessa, koska ne koskevat vain yhtä tiettyä riskienhallinnan osa-aluetta.

1.3 Tutkimusmetodologia

Tutkimus on luonteeltaan laadullinen case- eli tapaustutkimus, joka on tutkimusotteeltaan konstruktiivinen. Konstruktiivinen tutkimus kuuluu soveltavan tutkimuksen joukkoon. Soveltavan tutkimuksen tunnusmerkkeihin kuuluu tulosten relevanssi, yksinkertaisuus ja helppokäyttöisyys. Konstruktiivinen tutkimusote perustuu tosielämän ongelman ratkaisemiseen uudella ratkaisulla, konstruktiolla. Konstruktio voi olla muun muassa malli, suunnitelma tai järjestelmä. Konstruktion kehittämisen tarkoitus on luoda jotain uutta. (Kasanen, Lukka & Siitonen 1993, 243, 245) Konstruktiivinen tutkimusote yhdistää teoreettista ja empiiristä tietoa pyrkiessään rakentamaan innovatiivisen, teoreettisesti perustellun, toimivan ratkaisun empiirisen maailman ongelmiin (Kihn & Näsi 2011, 66). Konstruktiivisessa tutkimuksessa rakennetun konstruktion toimivuutta tulisi testata (Kasanen, Lukka & Siitonen 1993, 246).

Tapaustutkimus on laadullisen tutkimuksen yleisin tutkimusmuoto (Gummesson 2000, 83). Case-tutkimuksella tarkoitetaan sellaista tutkimusta, jossa tutkimuksen kohteena on yksi tai enintään muutama tietyllä tavalla valittu tapaus, joka voi olla esimerkiksi jokin yritys, yrityksen osa tai prosessi. Tässä tutkimuksessa tapaus on yrityksen järjestelmä, Pirkanmaan Osuuskaupan riskienhallintajärjestelmä. Tapaustutkimuksen tulokset eivät

[1] Katso lisää esim. http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx; http://www.iso.org/iso/catalogue_detail?csnumber=39612
http://www.iso.org/iso/catalogue_detail?csnumber=39612
[2] ISO (The International Organization for Standardization) on globaali kansallisten standardiorganisaati-

ole suoraan yleistettävissä tutkimuskohteen ulkopuolelle, vaan ne muodostavat aina tietyn ilmiön mahdollisimman totuudenmukaisen kuvauksen. Tapaustutkimuksen tavoitteena onkin kuvailla tutkittavaa ilmiötä, ymmärtää sitä syvällisemmin sekä tuottaa siitä yksityiskohtaista ja kokonaisvaltaista tietoa. (Hirsjärvi, Remes & Sajavaara 2009, 134–135; Eriksson & Kovalainen 2008, 117) Tapaustutkimuksen hyötyjä ovat tutkimuksen spesifisyys ja tapauksen kokonaisvaltainen ymmärtäminen realistisesti kuvatussa ympäristössä (Koskinen, Alasuutari & Peltonen 2005, 154–156).

Tutkimuksessa pyritään siis luomaan konstruktio kohdeyrityksen riskienhallintajärjestelmään. Konstruktio perustuu aiempaan kirjallisuuteen sekä haastatteluin kerätyn aineiston analyysiin. Tutkimuksen puitteissa ei kuitenkaan ole mahdollista implementoida ja arvioida kehitetyn konstruktion toimivuutta yrityksen toiminnassa, sillä riskienhallintajärjestelmän muuttaminen on pitkäkestoinen prosessi. Tutkimuksen tekijän ymmärryksellä ja tulkinnoilla onkin merkittävä vaikutus tutkimuksen päätelmiin ja lopputuloksiin.

2 RISKIENHALLINTA KIRJALLISUUDESSA

2.1 Riskienhallinnan määritelmä ja motiivit

Standardit riskienhallinnan määritelmän taustalla

Organisaatioiden riskienhallinnan työtä helpottamaan on luotu useita niin kansallisia kuin kansainvälisiäkin standardeja, jotka tarjoavat sekä yleisiä että tietyille toimialoille nimenomaisia malleja, joilla riskejä voidaan hallita. Ensimmäinen riskeihin liittyvä standardi oli norjalainen standardi *NS5814:1991: Krav til risikoanalyser* (Norges Standardiseringsforbund, 1991), joka käsitteli kuitenkin vain riskianalyysia. Uudempia, kansallisia standardeja ovat muun muassa japanilainen JIS Q2001:2001(E) ja brittiläinen BS 6079-3:2000. (Raz & Hillson 2005, 53–54) Tässä tutkimuksessa on hyödynnetty standardeja, joita yleisluonteisuutensa puolesta voidaan hyödyntää toimialasta riippumatta niin julkisella kuin yksityiselläkin sektorilla: ISO 31000:2009, AS/NZS 4360:2004 ja The Risk Management Standard. Kansainvälinen riskienhallinnan standardi, *ISO 31*000[2], julkaistiin vuonna 2009. Sen suunnittelussa hyödynnettiin jo aikaisemmin Australian ja Uuden-Seelannin standardiorganisaatioiden laatimaa riskienhallinnan standardia *AS/NZS 4360:2004*. (AS/NZS ISO 31000:2009 2009, 2) Britanniassa vuonna 2002 julkaistu riskienhallinnan standardi, *The Risk Management Standard*, on puolestaan riskienhallinnan ammattiorganisaatioiden laatima[3], jonka Federation of European Risk Management Associations (FERMA) vuotta myöhemmin virallisesti hyväksyi.

ISO 31000 standardi (2009, 1), Australian ja Uuden-Seelannin riskienhallintastandardi (AS/NZS 4360:2004, 4) sekä The Risk Management Standard (AIRMIC, ALARM & IRM 2002, 2) määrittelevät riskin epävarmaksi tapahtumaksi, jolla voi olla sekä negatiivisia että positiivisia seurauksia. Riski voi siis muodostua paitsi siitä, että epävarma ta-

[2] ISO (The International Organization for Standardization) on globaali kansallisten standardiorganisaatioiden yhteenliittymä.
[3] The Risk Management Standardin laatimiseen osallistuivat The Institute of Risk Management (IRM), The Association of Insurance and Risk Managers (AIRMIC) ja The National Forum for Risk Management in the Public Sector (ALARM).

pahtuma realisoituu ja aiheuttaa organisaatiolle vahinkoa myös siitä, että mahdollisuus, jolla voitaisiin saavuttaa organisaation asettamat tavoitteet, jätetään hyödyntämättä. Riskienhallinta käsittää näiden standardien mukaan toimintakulttuurin, prosessit ja rakenteet, jotka edesauttavat potentiaalisiin mahdollisuuksiin tarttumista sekä auttavat hallitsemaan haitallisia tapahtumia. Riskienhallinta on siten haitallisten tapahtumien välttämisen tai niiden seurausten pienentämisen lisäksi myös potentiaalisten mahdollisuuksien tunnistamista, analysointia ja hyödyntämistä organisaation tavoitteiden saavuttamiseksi. (AS/NZS 4360:2004, 5, 25; ISO 31000:2009, 2–3; AIRMIC, ALARM & IRM 2002, 2)

Riskienhallinnan motiivit

Uuden tiedon määrä on valtava nyky-yhteiskunnassa. Tieto ei kuitenkaan ole koskaan täydellisen varmaa ja hyvinkin varmana pidetty tieto on varmaa vain siihen saakka, kunnes uudet tutkimustulokset kyseenalaistavat vanhat teoriat. Tiedon epävarmuus ja erilaisten vaihtoehtojen lukematon määrä aiheuttavatkin riskejä, joiden hallitsemiseksi organisaatioiden tulee tehdä erilaisia toimenpiteitä. (Giddens 1991, 3–4) Epävarmuutta lisääviä tekijöitä ovat ympäristön monimutkaisuus, globaalit markkinat sekä teknologiset muutokset, jotka moninkertaistavat organisaation kohtaamien riskien määrän sekä vaikeuttavat niiden tunnistamista ja seurantaa (The Economist Intelligence Unit 2007, 6) Epävarmuutta ei voida tarkastella asia kerrallaan, vaan riskienhallinnassa tulee huomioida asioiden ja epävarmuuksien yhteydet toisiinsa ja näin pyrkiä hallitsemaan kokonaisuuksia (Stirling 1998, 98).

Monimutkainen ja epävarma ympäristö on aiheuttanut myös sen, että organisaation ulkopuoliset sidosryhmät vaativat yhä läpinäkyvämpää ja tehokkaampaa riskienhallintaa. Riskienhallintaan kohdistetut säännöt ja määräykset vaativat organisaatioita panostamaa resursseja yhä enemmän riskienhallintaan. Lisäksi sijoittajat ovat organisaatioiden taloudellisen epävarmuuden kasvun myötä yhä kiinnostuneempia siitä, miten organisaatioiden riskienhallintaa todellisuudessa hoidetaan. Monet organisaatiot ovat vastanneet näihin ulkoisiin paineisiin muun muassa parantamalla viestintää riskienhallintansa tilasta organisaation ulkopuolelle. Organisaation sisäisistä toimijoista riskienhallintaan vaikuttaa eniten hallitus. Hallituksen sitoutumista riskienhallintaan pidetään tärkeänä moti-

vaation luojana pyrittäessä tehokkaamman ja toimivamman riskienhallinnan järjestämiseen. (PwC 2008, 3; The Economist Intelligence Unit 2007, 2, 6–7)

Epävarmuuden ja tulevaisuuden absoluuttisen ennustamisen mahdottomuuden vuoksi organisaatioiden on pakko turvautua edes jonkin asteiseen riskienhallintaan varmistaakseen organisaation toiminnan jatkuvuuden (Shenkir & Walker 2007, 1).The Economist Intelligence Unitin tekemän tutkimuksen (2007, 2–3) mukaan ympäristön ja markkinoiden muuttuminen näkyy riskienhallinnan motiiveissa. Riskienhallinnan tavoitteena ei ole enää vain välttää tappioita, vaan yhä enemmän huomio kiinnittyy maineen suojeluun ja parantamiseen sekä kilpailuedun saavuttamiseen.

Riskienhallinnalla pyritään siis paitsi varautumaan liiketoiminnallisilta uhilta ja pitämään riskit riskinottohalukkuuden rajoissa myös hyödyntämään liiketoiminnan sisäiset ja ulkoiset mahdollisuudet (Blumme ym. 2005, 79). Ne, jotka havittelevat suuria voittoja, joutuvat altistamaan toimintansa huomattavalle riskille. Yhteys riskin ja voiton välillä on ilmeinen esimerkiksi sijoittamisen yhteydessä; osakkeet ovat riskisempiä kuin valtion obligaatiot, mutta ne myös todennäköisesti tuottavat pitkässä juoksussa enemmän. Liiketoiminnan menestymisen kannalta riskeihin suhtautuminen on ratkaisevassa roolissa. Organisaatio, joka suojelee itseään kaikilta riskeiltä, tuottaa todennäköisesti hyvin vähän omistajille lisäarvoa. Toisaalta jos organisaatio altistaa toimintansa vääränlaisille ja liian suurille riskeille eikä näin kykene kantamaan mahdollisia riskin negatiivisia seurauksia, on lopputulos usein vieläkin huonompi. Osana riskienhallintaa tuleekin määritellä, kuinka paljon organisaatio on kykenevä ja halukas riskiä ottamaan. Tehokkaan ja järjestelmällisen riskienhallinnan avulla suurempien riskien ottaminen hallitusti mahdollistuu ja näin myös suurempien voittojen tekeminen on todennäköisempää. (Chapman 2001, 32; COSO 2004, 3,13, 19; Damodaran 2008, 7; Kyrölä 2010, 62; Rappaport 1998, 1; Shenkir & Walker 2007, 1) Lisäarvon tuottaminen sidosryhmille, erityisesti sijoittajille, onkin tulos onnistuneesta riskinotosta (Blumme ym. 2005, 79; Fraser & Simkins 2010, 4).

Organisaatioiden ympäristön sekä niiden riskienhallinnan luonteen muuttuminen on aiheuttanut sen, että riskienhallinnalle asetetaan yhä kovempia tulospaineita. Organisaatiot haluavat varmistua, että tehdyillä investoinneilla riskienhallintaan todella saavutetaan lisäarvoa. Riittäväksi lisäarvoksi ei enää katsotakaan vain sitä, että vahinko tai menetys

olisi tapahtunut ilman riskienhallintaa, vaan hallitus ja sijoittajat haluavat tietää, mitä aineellista lisäarvoa sillä on saatu aikaan. (The Economist Intelligence Unit 2007, 12) Riskienhallinnan pitääkin lisätä organisaation toimintojen arvoa, jotta siihen ollaan valmiita panostamaan ja sitoutumaan organisaatiossa (AIRMIC, ALARM, IRM 2002, 2).

2.2 Riskienhallintaprosessi

Riskienhallintaprosessilla tarkoitetaan jatkuvaa prosessia, jossa organisaation toiminnasta aiheutuvia ja siihen olennaisesti liittyviä riskejä tunnistetaan, analysoidaan, priorisoidaan, hallitaan ja seurataan (kuvio1) (Blumme ym. 2005, 79; COSO 2004, 17; Kupi, Keränen & Lanne 2009, 11). Riskienhallintaa ei ole tarkoitus toteuttaa yksittäisenä kertaluonteisena projektina tai vaiheittain edeten. Organisaatioiden toimintaympäristö on jatkuvan muutoksen alla, eikä kaikkia riskejä kyetä tunnistamisvaiheessa määrittelemään, joten organisaatiossa voi olla useampikin kuviossa 1 esitetyn prosessimallin vaiheesta samanaikaisesti käynnissä (AIRMIC, ALARM & IRM 2002, 2; COSO 2004, 17; Suominen 2003, 30–31).

Hyvä riskienhallinta on tietoista, suunnitelmallista ja järjestelmällistä toimintaa (Malmén & Wessberg 2011). Järjestelmällinen toiminta vaatii paitsi kommunikointia ja viestintää organisaation sisällä, myös ohjeistuksen siitä, miten riskienhallintaa tulisi toteuttaa. Riskienhallintaprosessin mallikaaviota voidaan hyödyntää ohjeistuksen laadinnassa. Riskienhallintaprosessin mallit ovat kuitenkin vain kuvauksia niistä riskienhallinnan päävaiheista, joita organisaation riskienhallintaprosessiin tulisi sisällyttää. Mallien tarkoituksena onkin lähinnä tarjota lähtökohtia riskienhallinnan kehittämiselle sekä riskien yhdenmukaiselle, kontrolloidulle tarkastelulle ja hallitsemiselle. (Kupi, Keränen & Lanne 2009, 17)

Riskienhallinnan lähtökohtana on riskienhallintapolitiikka ja strategia suhtautumisesta riskeihin. Riskienhallintapolitiikassa linjataan riskienhallinnan strategiset tavoitteet. Riskistrategia puolestaan ohjaa tekemään yhdenmukaisia ratkaisuja; siitä selviää, mitä riskejä organisaatiossa halutaan hyödyntää, mitä puolestaan halutaan välttää ja kuinka paljon riskiä ollaan valmiita ottamaan sekä, kuinka paljon tuottoa halutaan riskillä saa-

vuttaa. Riskistrategia toisin sanoen vaikuttaa paitsi organisaation tapaan suhtautua riskeihin myös kaikkeen päätöksentekoon. (Buehler & Pritsch 2003, 43; COSO 2004, 22–23) Koska riskienhallintaprosessi voi olla samanaikaisesti useammassa yksikössä käynnissä, ovat yhteiset riskienhallinnan tavoitteet ja käsitteet välttämättömiä, jotta vältytään osaoptimoinnilta ja riskienhallinnan pirstaleisuudelta (PwC 2008, 8–9).

Riskianalyysivaiheessa on tarkoitus paitsi tunnistaa kaikki organisaation toimintaan liittyvät riskit myös järjestelmällisesti arvioida näitä riskejä (Pwc 2008, 5). Jottei riskien analyysivaihe olisi vain sattumanvaraista riskien arviointia, tulisi organisaatiolla olla selkeä ohjeistus siitä, miten riskejä tunnistetaan, analysoidaan ja arvioidaan. (Malmén & Wessberg 2011, 2) Riskien tunnistaminen vaatii valmiiden toimintamallien lisäksi perinpohjaista organisaation ja sen toimintaympäristön tuntemista sekä operatiivisten ja strategisten tavoitteiden ymmärtämistä. Riskien tunnistamista ohjaa organisaation toiminnot, joista riskit johtuvat. (AIRMIC, ALARM & IRM 2002, 5) Riskit voivat olla hyvinkin erilaisia ja monimutkaisia, joten on tarpeellista käyttää useampia riskien tunnistamistekniikoita, jotta mahdollisimman moni riski tulee tunnistetuksi. [4] Riskit, jotka jäävät tunnistamatta altistavat liiketoiminnan yllättäville uhille ja toisaalta liiketoiminnallisia mahdollisuuksia voi tämän seurauksena jäädä hyödyntämättä. (Shenkir & Walker 2011, 14)

Tunnistettujen riskien analysoinnilla lisätään riskeihin liittyvää tietoa muun muassa riskien todennäköisyyksistä, niiden seurauksista sekä syistä. Riskiarvioinnin ja -priorisoinnin kautta organisaatiossa luodaan parempi käsitys siitä, miten riskienhallintaa tulisi toteuttaa ja, miten riskienhallinnan resurssit on tarkoituksenmukaisinta jakaa. Riskejä arvioitaessa tulee selvittää, mihin organisaation riskeistä on mahdollista vaikuttaa ja, ovatko riskit ylipäänsä sellaisia, että niihin halutaan vaikuttaa. (Kupi, Keränen & Lanne 2009, 19; PwC 2008, 6; Shenkir & Walker 2011, 16)

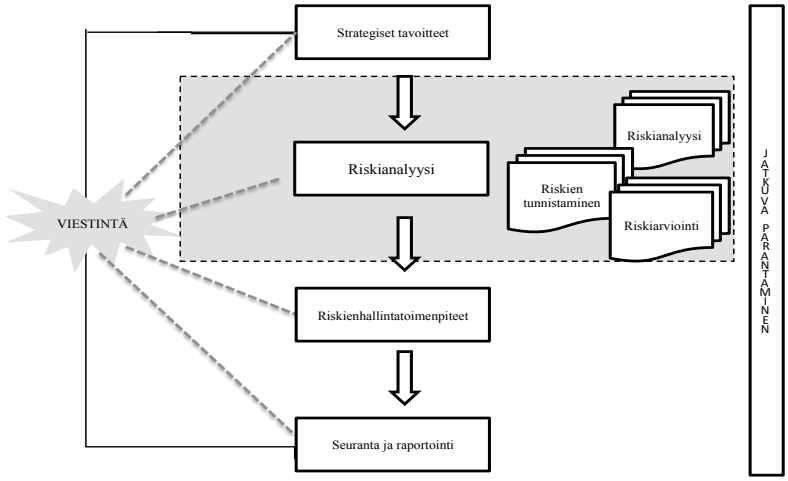
Riskianalyysin, riskienhallintapolitiikan ja riskistrategian pohjalta organisaatio arvioi tapoja, joilla se voi riskejään hallita (PwC 2008, 31). Riskienhallintatoimenpiteiden valintaan vaikuttaa paitsi tarvittavien resurssien määrä myös se, millaisia seurauksia toimenpiteillä arvioidaan saatavan aikaan. Riskienhallintatoimenpiteiden tulee olla sellai-

[4] Erilaisia riskien tunnistamistekniikoita on käsitelty muun muassa IMA:n lausunnossa *Enterprise Risk Management: Tools and Techniques for Effective Implementation.* (2007).

sia, että riskienhallinnasta aiheutuvat kustannukset ovat järkevät saataviin hyötyihin verrattuna. Lisäksi riskienhallinnan toimenpiteiden tavoitteena on asettaa organisaation kokonaisriski, joka jää jäljelle, organisaation riskinottohalua vastaavaksi. Riskienhallintatoimenpiteet, joita kirjallisuudessa yleensä esitetään, ovat: riskin välttäminen, pienentäminen, siirtäminen ja hyväksyminen. (Shenkir & Walker 2011, 18) Edellä esitetyissä riskienhallinnan toimenpiteissä riskienhallinta nähdään vain haitallisten tapahtumien välttämisenä tai niiden seurausten pienentämisenä. Riskienhallintatoimenpiteiden arvioinnin yhteydessä, tulee kuitenkin huomioida myös potentiaaliset mahdollisuudet, jotka halutaan organisaatiossa mahdollisesti hyödyntää. Menestyäkseen organisaatioiden tulee ymmärtää riskienhallinnan täydellinen kuva, jossa huomioidaan riskit, joilta pitää suojautua, mutta myös ne mahdollisuudet, joiden hyödyntämättä jättäminen on riski sinänsä. Lisäksi organisaatiolla pitää tietenkin olla ymmärrys siitä, miten näitä mahdollisuuksia voidaan hyödyntää. (Buehler, Freeman & Hulme 2008, 104; Damodaran 2008, 9–10)

Riskienhallintaprosessin seurannan avulla varmistutaan, että prosessi toteutuu joka vaiheessa niin kuin on suunniteltukin. Lisäksi mitataan tehtyjen toimenpiteiden vaikuttavuutta ja arvioidaan ympäristön muutosten vaikutusta organisaation riskeihin ja riskienhallintaan. Seuranta mahdollistaa jatkuvan riskienhallintaprosessin kehittämisen. (Shortreed 2010, 8)

Viestintä, jolla varmistetaan riittävä sisäinen ja ulkoinen tiedonkulku, on oleellisessa osassa kaikissa riskienhallintaprosessin vaiheissa. Riskienhallinnasta tulee viestiä useille eri sidosryhmille, kuten henkilöstölle, viranomaisille ja omistajille. Palautekanavien sidosryhmistä organisaatioon päin tulee myös olla toimivat. (AS/NZS 4360:2004, 11; Kupi, Keränen & Lanne 2009, 20) Raportointi riskienhallintaprosessin etenemisestä ja onnistumisesta on myös yksi riskienhallinnan jatkuvan parantamisen lähtökohdista (COSO 2004, 22–23).



Kuvio 1 Riskienhallintaprosessi (mukaillen julkaisuista AS/NZS 4360:2004, 7–9; A Risk Management Standard 2002, 4; COSO 2004, 22; ISO 31000:2009 ja Shenkir & Walker 2007, 2)

2.3 Kokonaisvaltaisen riskienhallinnan ajatusmalli

Riskienhallinta on perinteisesti ollut riskilajeihin jakautunutta, jolloin riskejä on tarkasteltu omissa luokissaan, toisista riskiluokista erillään. Organisaatioiden ja ympäristön monimutkaisuuden kasvun ja globalisaation myötä organisaatiot ovat kuitenkin ymmärtäneet riskien kokonaistarkastelun merkityksen. Kokonaisvaltainen riskienhallinta (Enterprise Risk Management, ERM) on malli, joka auttaa tarkastelemaan riskejä holistisesti sekä lisää ymmärrystä riskien keskinäisistä riippuvuussuhteista. (Ai, Brockett, Cooper & Golden 2012, 29; McShane, Nair & Rustambekov 2011, 644; Shenkir & Walker 2011, 4) Kokonaisvaltaisen riskienhallinnan ajatuksen mukaan riskienhallinta koskee koko organisaatiota, kattaa kaikki riskikategoriat ja tavoittelee integraatiota kaikkien johdon toimintojen kanssa (Kimbrough & Componation 2009, 19).

Kokonaisvaltainen riskienhallinta on kansainvälisesti hyväksytty kasvava konsepti, josta on esitetty useita erilaisia viitekehyksiä ja lausuntoja. Osa viitekehyksistä on pakottavia, osa niin sanottuja comply or explain -malleja ja osan on puolestaan tarkoitus toimia tukena kokonaisvaltaisen riskienhallinnan käyttöönotossa ja toteuttamisessa. Viitekehykset ovat lähestymistavoiltaan erilaisia ja näin ne soveltuvatkin eri alojen organisaatioiden käyttöön ERM:n soveltamisen tueksi. Tunnetuimpia ERM viitekehyksiä ovat:

- A Risk Management Standard by the Federation of European Risk Management Association
- Australian/New Zealand Standard 4360 – Risk Management
- COSO's Enterprise Risk Management – Integrated Framework
- Basel II
- Standard & Poor's and ERM

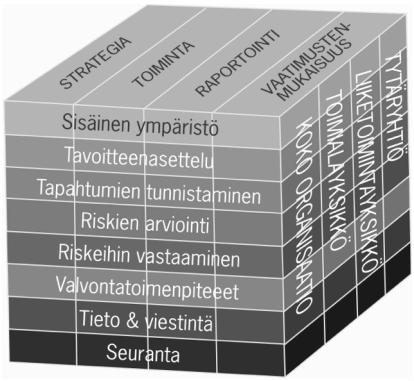
Näistä Basel II ja Standard & Poor's and ERM koskevat ainoastaan rahoitus- ja vakuutussektoria. (Shenkir &Walker 2011, 7–8)

Kokonaisvaltaista riskienhallintaa voidaan pitää yleisnimityksenä riskienhallinnasta, jonka taustalla on ajatus siitä, että riskienhallintaan tulisi kehittää kattavampia välineitä ja toimintamalleja, joilla pystyttäisiin paremmin käsittelemään riskienhallintaan kohdistuvia yhteiskunnan ja ympäristön luomia ulkoisia paineita (Räikkönen & Rouhiainen 2003, 8). COSO (2004, 16) on määritellyt kokonaisavaltaisen riskienhallinnan yleisluonteisesti:

> Organisaation riskienhallinta on sen hallituksen, johdon ja muun henkilökunnan toteuttama prosessi, jota sovelletaan strategian laadinnassa ja koko organisaatiossa, ja jonka tarkoituksena on tunnistaa organisaatioon vaikuttavia potentiaalisia tapahtumia ja pitää riskit riskinottohalukkuuden rajoissa, jotta voidaan olla kohtuullisen varmoja organisaation tavoitteiden toteutumisesta.

COSO:n (2004, 23) muotoilemassa kolmiulotteisessa kuutiomatriisissa (kuvio 3) kiteytyy kokonaisvaltaisen riskienhallinnan ero perinteiseen riskienhallintaan. Kuutiomatriisissa on riskienhallinnan osa-alueiden lisäksi esitetty organisaation tavoitekategoriat ja yksiköt. Muutos niin sanottuun perinteiseen riskienhallintaan syntyykin siitä, että riskienhallintaprosessi liitetään osaksi organisaation eri tavoitekategorioita ja sen yksiköiden toimintaa. Kuutiomatriisilla pyritään kuvaamaan organisaation riskienhallintaprosessin luonnetta, joka on monisuuntainen ja toistuva, ja jossa lähes kaikki osa-alueet vaikuttavat tai ainakin voivat vaikuttaa toisiinsa. Riskienhallinta on koko organisaation kattava prosessi, jonka tavoitteena on varmistaa organisaation tavoitteiden saavuttaminen. (COSO 2004, 17, 23) Kokonaisvaltaisessa riskienhallinnassa riskienhallinta kytketään yrityksen strategisiin, toiminnallisiin ja taloudellisiin tavoitteisiin, jolloin riskien tarkastelunäkökulma siirtyy yksittäisistä toiminnoista ja niihin liittyvistä riskeistä koko

yrityksen tasolle, ja riskienhallinnan keskeiseksi päämääräksi muodostuu yrityksen taloudellisen ja toiminnallisen kokonaishyödyn maksimointi riskienhallinnan keinoin. (Blumme ym. 2005, 84)



Kuvio 2 Riskienhallintamatriisi (COSO 2004, 23)

Hyvin toteutetun kokonaisvaltaisen riskienhallinnan etuja ovat riskienhallinnan tehostuminen, organisaation ja liiketoimintayksiköiden kokonaisriskin parempi ymmärtäminen, tehokas resurssien kohdentaminen liiketoimintayksiköille, riskitietoisuuden lisääntyminen organisaatiossa ja riskien huomioiminen kaikissa organisaation prosesseissa sekä kaikessa päätöksenteossa, mikä edesauttaa oikeaa päätöksentekoa. (Hoyt & Liebenberg 2011, 797; Rosa 2007, 50). Kokonaisvaltainen riskienhallinta on siis omiaan tehostamaan riskienhallintaa, mikä taas vaikuttaa positiivisesti kaikkeen organisaation toimintaan. Tehokkaan riskienhallinnan avulla organisaation johto muun muassa kykenee paremmin saavuttamaan tulos- ja kannattavuustavoitteensa. Lisäksi riskienhallinta auttaa varmistamaan tehokkaan raportoinnin sekä lakien ja määräysten noudattamisen ja näin voidaan välttää organisaation maineen vahingoittuminen ja siihen liittyvät seuraukset. Kaiken kaikkiaan kokonaisvaltainen riskienhallinta auttaa organisaatiota etenemään päämääräänsä ja välttämään yllättäviä tilanteita. (COSO 2004, 5)

3 RISKIENHALLINNAN ARVIOIMINEN

3.1 Sisäinen tarkastus riskienhallinnan tehokkuuden ja toimivuuden arvioijana

Riskienhallinnan tehokkuuden arvioiminen on tärkeää, jotta organisaation hallitus ja johto voivat olla kohtuullisen varmoja siitä, että heillä on oikeaa tietoa yrityksen tavoitteiden toteutumisen tilasta, organisaatio raportoi luotettavasti, ja että lakeja ja määräyksiä noudatetaan. (COSO 2004, 24) Arvioinnissa on kuitenkin myös kysymys jatkuvan parantamisen edistämisestä. Mikäli arvioinnin tuloksena saadaan tietoon, että riskienhallinta ei vastaa asetettuja tavoitteita, voidaan toimintaa muuttaa tavoitteiden saavuttamiseksi. Arviointia voidaan siis pitää myös muutokseen johtavana kehittämisen keinona. (Lindow & Race 2002, 28)

Jotta riskienhallinnan arviointi olisi mahdollisimman objektiivista, tulisi tehtävää hoitavan tahon olla organisaatioon nähden riippumaton. Näin ollen sisäinen tarkastus toimiikin usein riskienhallinnan arvioijan roolissa. Se tekee organisaation riskienhallintaa koskevia arviointeja aina strategiatasolta prosessi-, toiminto-, projekti- ja tehtävätasolle. (Holopainen, Koivu, Kuuluvainen, Lappalainen, Leppiniemi, Mikola & Vehmas 2006, 15, 36, 66; IIA 2009, 3) Riskienhallinnan tehokkuuden ja riittävyyden arvioinnin lisäksi sisäinen tarkastus toimii usein myös aktiivisena johdon keskustelukumppanina ja sparraajana (Sobel & Kapoor 2012, 43).

Sisäistä tarkastusta voidaan pitää organisaation perustoimintona, vaikka läheskään kaikista organisaatioista erillistä sisäisen tarkastuksen funktiota ei löydykään. Tehtävää saattaakin hoitaa esimerkiksi kontrollerin tehtäviä hoitava henkilö. Lopullinen vastuu riskienhallinnan järjestämisestä ja sen riittävyydestä on hallituksella, tarkastusvaliokunnalla tai sitä vastaavalla toimielimellä. Sisäisen tarkastuksen perustamisen osalta tulisikin harkita sitä, onko organisaatio niin suuri ja toiminnaltaan monimutkainen, että hallitus tarvitsee avukseen joko oman tai ostopalveluilla toimivan sisäisen tarkastuksen yksikön. Tämä tietenkin koskee kuitenkin vain niitä organisaatioita, joilla on mahdollisuus

itse valita sisäisen tarkastuksen järjestämisestä. Esimerkiksi luottolaitoksilla ja sijoituspalveluyrityksillä on lakiin perustuva velvollisuus riippumattoman riskienhallinnan arviointitoiminnon järjestämisestä. (Finanssivalvonta, standardi 4.1, 14; Holopainen ym. 2006, 71, 79)

Mikäli sisäisen tarkastuksen lakisääteistä järjestämistä ei oteta lukuun, sisäisen tarkastuksen järjestämisen motiivit löytyvät sekä organisaation sisältä että sen ulkopuolelta. Sisäisen tarkastuksen avulla johto ja hallitus saavat kohtuullisen varmuuden siitä, että merkittävimmät riskit on huomioitu ja niitä hallitaan tehokkaasti ja johdonmukaisesti siten, että asetetut tavoitteet voidaan saavuttaa. (ISO 31000:2009, 5) Lisäksi sisäistä tarkastusta kohtaan asetetut ulkoiset odotukset ovat kasvaneet huomattavasti muun muassa riskienhallinnan pettämisen ja tilintarkastusten epäonnistumisten myötä (Holopainen ym. 2006, 102).

Arvioinnin lähteet ja perusteet

Jotta riskienhallinnan tehokkuutta ja tarkoituksenmukaisuutta voitaisiin arvioida, tulee olla arviointiperusteet tai -kriteerit, joihin arvioitavaa kohdetta voidaan verrata. Arviointiperusteilla siis määritellään, miten ja mitä vasten toimintaa mitataan. Arviointiperusteet voivat olla lähtöisin organisaation sisältä. Riskienhallinnan toteutumia voidaan verrata esimerkiksi organisaation arvoihin, strategiaan, visioon, toimintasuunnitelman tai budjettiin. Vaihtoehtoisesti arviointiperusteina voidaan käyttää organisaation ulkopuolelta johdettuja kriteereitä, kuten lait, säädökset tai yleisesti hyväksytyt standardit. (Holopainen ym. 2006, 254–255) Kuten riskienhallintaprosessi myös sen arviointiprosessi tulee suunnitella ja toteuttaa yksilöllisesti organisaation tarpeisiin (IIA 2010, 10).

COSO:n julkaiseman kokonaisvaltaisen riskienhallinnan viitekehyksen kahdeksaa osa-aluetta voidaan hyödyntää riskienhallinnan tehokkuuden ja riittävyyden arvioinnissa. Jos kaikki sen osa-alueet ovat olemassa ja niitä toteutetaan asianmukaisesti, tällöin organisaation riskienhallinnassa ei pitäisi olla materiaalisia heikkouksia, ja riskien tulisi pysyä riskinottohalukkuuden rajoissa. Viitekehys toimiikin organisaatioille mallina, jolla voidaan paitsi parantaa organisaation sisäistä valvontaa myös kehittää riskienhallintaa yhä kokonaisvaltaisemmaksi. (COSO 2004, 3, 7)

Riskienhallinnan laatustandardin *ISO 31000* mukaista riskienhallintaa voidaan pitää riskienhallinnan parhaana käytäntönä. Siinä esitetään riskienhallinnan viitekehys, periaatteet ja prosessit, joita organisaatioissa tulisi noudattaa, jotta ne voisivat paremmin saavuttaa tavoitteensa. (ISO 31000:2009; Shortreed 2010, 8) Standardia voidaan hyödyntää niin riskienhallinnan politiikkaa kehitettäessä kuin riskienhallinnan tehokkuutta arvioitaessakin (ISO 31000:2009, 6). Lisäksi The Institute of Internal Auditors (IIA) on julkaissut ISO 31000 standardin pohjalta oppaan *Assessing the Adequacy of Risk Management – Using ISO 31000,* jossa esitetään kolme erilaista mallia riskienhallinnan arviointiin: prosessi-, avainperiaate- ja kypsyysmalli. Prosessimallin mukaan riskienhallintaa voidaan arvioida sen perusteella, löytyykö organisaation riskienhallinnasta kaikki ne riskienhallintaprosessin osatekijät, joita yleiset riskienhallinnan viitekehykset edellyttävät. Avainperiaatemallilla tarkoitetaan sitä, että organisaation riskienhallinnan tulee täyttää tietyt periaatteet, jotta se voisi olla tehokasta. Kypsyysmalli puolestaan rakentuu ajatukselle, että riskienhallintaprosessi kehittyy ajassa ja riippuen siitä, missä kohtaa maturiteettikäyrää organisaatio on, tulisi sen täyttää tietyt odotukset. Nämä lähestymistavat ovat toisistaan riippumattomia ja ne tarjoavatkin kaikki erilaisen näkökulman riskienhallinnan prosessin arviointiin. Luonnollisesti useampaa mallia käyttämällä saadaan informatiivisempia tuloksia kuin vain yhden lähestymistavan avulla. (IIA 2010, 10–11)

IIA on lisäksi julkaissut sisäisen tarkastuksen kansainväliset ammattistandardit - *International Standards for the Professional Practice of Internal Auditing*, joista tuli voimaan uudistunut versio vuoden 2011 alusta. Ammattistandardit ovat sisäisen tarkastuksen luonnetta ja toteutusta kuvaavia keskeisiä periaatteita ja ne ovat luonteeltaan velvoittavia. (Halla, Hätinen, Grönfors-Kallio, Malm, Kaisanlahti, Kontula & Väisänen 2003, 18) Standardissa 2120 todetaan sisäisen tarkastuksen rooli osana riskienhallintaa: *”Sisäisen tarkastuksen toiminnon tulee arvioida riskienhallintaprosessin tuloksellisuutta ja edistää niiden kehittämistä.”* Standardissa eritellään myös periaatteet, joihin arvioinnin tulee nojata:

- Organisaation tavoitteiden tulee olla linjassa organisaation toiminta-ajatuksen kanssa;
- Keskeiset riskit on tunnistettu ja arvioitu;

- On valittu sellaiset tarkoituksenmukaiset riskienhallintakeinot, joilla voidaan varmistua, että riskit ovat linjassa organisaation hyväksytyn riskinottotason kanssa;
- Olennainen tieto riskeistä on kerätty ja raportoitu organisaation sisällä ajantasaisesti siten, että henkilökunta, johto ja hallitus voivat suoriutua heille asetetuista velvollisuuksista. (Sisäiset tarkastajat ry 2010, 13)

Näitä standardin 2120 arviointiperusteita täydentämään seuraavassa on esitetty vielä muita riskienhallinnan arviointiperiaatteita:

- Riskienhallinta luo ja säilyttää arvoa;
- Riskienhallinta perustuu riskienhallintapolitiikkaan;
- Riskienhallinnan tavoitteet ovat selkeät;
- Riskienhallinta on olennainen osa organisaation prosesseja;
- Riskienhallinta on mukana päätöksenteossa;
- Riskienhallinnan vastuut on eritelty;
- Riskienhallinnalla voidaan tunnistaa epävarmuuden aiheuttajat;
- Riskienhallinta on systemaattista, jäsenneltyä ja oikea-aikaista;
- Riskienhallinta perustuu parhaaseen saatavilla olevaan tietoon;
- Riskienhallinta on organisaation tarpeisiin räätälöityä;
- Riskienhallinnassa huomioidaan kulttuuritekijät;
- Riskienhallinta on läpinäkyvää ja täydellistä;
- Riskienhallinta on dynaamista ja muutoksen huomioivaa;
- Riskienhallinnasta on viestitty riittävällä tasolla organisaatiossa;
- Riskienhallinta on mukana jatkuvan parantamisen toteuttamisessa. (IIA 2010, 11; ISO 31000:2009, 7–10, 12)

Arviointiperusteita tarkasteltaessa huomataan, että sisäisen tarkastuksen riskienhallinnan kriteerit noudattelevat hyvin pitkälti kokonaisvaltaisen riskienhallinnan ajatusmaailmaa. Kokonaisvaltaista riskienhallintaa voidaankin näin pitää sisäisen tarkastuksen näkökulmasta tehokkaana riskienhallinnan toteuttamisen tapana.

3.2 Toimivan ja tehokkaan riskienhallintajärjestelmän malli

Edellisessä alaluvussa esitettyjen arviointiperusteiden sekä alan tutkimusten ympärille luodaan seuraavassa sellainen yleinen riskienhallintajärjestelmän malli, jota voidaan pitää sisäisen tarkastuksen arviointikriteerit täyttävänä ja näin myös tarkoituksenmukaisena tapana järjestää riskienhallinta organisaatiossa.

Kuten arviointiperusteissa todettiin, arvioi sisäinen tarkastus riskienhallintaa muun muassa sen perusteella, löytyykö organisaation riskienhallintaprosessista kaikki yleisten viitekehysten edellyttämät komponentit. Tutkimuksen kappaleessa 2.2 esitetty riskienhallintaprosessi tarjoaakin riskienhallintaprosessin mallin, jota organisaatiot voivat soveltaa omassa toiminnassaan ja näin täyttää sisäisen tarkastuksen asettamat vaatimukset prosessille. Riskienhallinnan arvioinnissa ei pidä kuitenkaan pelkästään keskittyä riskienhallinnan prosessiin, vaan riskienhallinta tulee nähdä arvioinneissa organisaation kokonaisuuden osana. Arvioinneissa huomio kiinnittyykin yhä enemmän riskienhallinnan yhdistämiseen organisaation muuhun toimintaan. Riskienhallintaprosessi tulisi sitoa organisaation strategia- ja suunnitteluprosessiin, liiketoiminnan päivittäiseen toteutukseen sekä normaaleihin liiketoiminnan seuranta- ja raportointimenetelmiin (Leino, Steiner & Wahlroos 2005, 136). Riskienhallintaosaamisen luontevaa kytkemistä johdon työhön ja päätöksentekoon voidaankin pitää hyvän johtamisen tunnusmerkkinä (Suominen 2005, 163).

3.2.1 Riskienhallinta osana organisaatiokulttuuria

Organisaatiokulttuuri on merkittävässä roolissa kaikessa organisaation toiminnassa. Yritysskandaaleista on syytetty muun muassa organisaatiokulttuurin toimimattomuutta. Kulttuurin merkitys kokonaisvaltaisen riskienhallinnan käyttöönotossa ja toteuttamisessa on myös tunnistettu merkittäväksi. Miccolis (2003) on esittänyt organisaatiokulttuurin olevan yksi suurimmista esteistä kokonaisvaltaisen riskienhallinnan käyttöönotossa. Kokonaisvaltaisen riskienhallinnan viitekehyksissä kulttuuri on osa sitä kokonaisuutta, josta riskienhallinnassa lähdetään liikkeelle. Kulttuuri yhdessä muiden tekijöiden kanssa luo pohjan muille riskienhallinnan osa-alueille. Viitekehyksissä käytetään muun muassa termejä kontekstin luominen (ISO 31000:2009, 10) ja sisäinen ympäristö (COSO 2004,

27). ISO:n viitekehyksessä huomioidaan sekä sisäinen että ulkoinen ympäristö, kun taas COSO:n viitekehyksessä riskienhallinnan järjestys ja rakenne muotoutuu organisaation sisäisen ympäristön ympärille. Kulttuuri puolestaan vaikuttaa siihen, millaiseksi organisaation sisäinen ympäristö muotoutuu.

Organisaatiokulttuurin yksiselitteinen määrittely on vaikeaa, ja eri alojen tutkijat ovatkin antaneet sille monenlaisia käsitteellisiä sisältöjä (ks. esim. Bate 1984; Pettigrew 1979; Schein 1987). Yleisesti organisaatiokulttuuri voidaan kuitenkin määritellä niiksi taidoiksi, käsityksiksi ja uskomuksiksi, arvoiksi, normeiksi sekä tavoiksi, jotka jokin yhteisö keskuudessaan jakaa. (Drew & Kendrick 2005, 28; Roche 2012; Virolainen 2010, 38) Sekä COSO:n että ISO:n mukaan riskienhallinta heijastaa näitä organisaation arvoja ja muita organisaatiokulttuurin tekijöitä, ja näin organisaatiokulttuuri vaikuttaa muun muassa siihen, kuinka riskejä tunnistetaan, mitä riskejä hyväksytään, miten riskejä hallitaan ja miten niistä tulee raportoida (COSO 2004, 27–28; ISO 31000:2009, 15) Organisaation virallisista politiikoista selviää, mitä hallitus ja johto toivovat tapahtuvan, mutta lopulta kuitenkin organisaatiokulttuuri on se, joka määrittää, mitä todella tapahtuu (COSO 2004, 30).

Kirjallisuudessa on esitetty useita erilaisia organisaatiokulttuurimalleja, joista osa tukee enemmän riskienhallinnan tehokasta toteuttamista ja osa vähemmän. Ronda Reigle on esittänyt vuonna 2001 organisaatiokulttuurin kaksi vaihtoehtoista mallia: *mekanistinen* ja *orgaaninen kulttuuri.* Mekanistinen kulttuuri on luonteeltaan virallinen, kontrolloitu ja hyvin jäsennelty; jokaisella organisaation jäsenellä on tarkoin määritelty tehtävä tiukassa, hierarkkisessa järjestelmässä. Orgaanisella tarkoitetaan puolestaan tässä yhteydessä sellaista organisaatiota, jossa ei ole tiukkaa normitusta, työtehtävät ovat löyhästi määritelty ja toiminta perustuu vuorovaikutukselle ja yhteistyölle ilman tiukkaa hierarkiaa. (Reigle 2001, 4) Vaikka mekanistinen kulttuuri kaikessa järjestelmällisyydessään vaikuttaisikin riskienhallinnan kannalta järkevältä vaihtoehdolta, on se kuitenkin riskien ja ympäristön monimutkaisuuden sekä nopeiden muutosten vuoksi usein luonteeltaan liian hidas riskienhallintaan. Lisäksi toimiva riskienhallinta vaatii avointa ja tehokasta kommunikaatiota ja yhteistyötä, joita mekanistinen kulttuuri on omiaan vähentämään. Orgaanista organisaatiokulttuuria pidetäänkin riskienhallinnan kannalta suotuisampana vaihtoehtona. (Kimbrough & Componation 2005, 48)

Reiglen määritelmästä voidaan löytää yhtäläisyyksiä organisaatiorakenteiden jaottelun kanssa. Organisaatiorakenteella tarkoitetaan sitä, miten tehtävät on jaettu organisaatiossa, kuka vastaa kenellekin toiminnastaan ja millaista vuorovaikutusta organisaatiossa on (Grunig 1992, 225). Organisaatiorakenteella voi olla vaikutusta kulttuuriin. Aivan kuten Reigle (2001, 4) määrittelee organisaatiokulttuurin orgaaniseksi tai mekanistiseksi voidaan organisaatiorakenteen sanoa olevan joko orgaaninen tai mekanistinen. Hyvin hierarkkinen organisaatiorakenne johtaakin usein mekanistiseen kulttuuriin. Sen sijaan päätöksenteon hajauttaminen ja organisaation johtaminen mahdollisimman paljon ilman johtajia johtaa orgaaniseen organisaatiokulttuuriin. (Grunig 1992, 225–226)

Vaikka riskien hallitseminen kokonaisuutena edellyttääkin avointa kommunikaatiota, yhteistyötä ja toiminnan läpinäkyvyyttä, voidaan kuitenkin kokonaisvaltaisen riskienhallinnan luonnetta tarkasteltaessa löytää myös piirteitä, jotka ovat luonteeltaan enemmän mekanistisen kulttuurin mukaisia. Kuten edellä on esitetty, kokonaisvaltaisen riskienhallinnan toteuttaminen perustuu täsmällisen prosessin noudattamiseen. Riskejä tunnistetaan, analysoidaan, priorisoidaan, valvotaan ja kontrolloidaan ennalta määritellyillä tavoilla. Lisäksi organisaatiossa tulisi vallita yhteinen kieli riskeistä, mikä on omiaan yhdenmukaistamaan riskienhallintaa. Toimiva riskienhallinta siis edellyttääkin vapaan ilmapiirin lisäksi, rutiininomaista toimintaa, joka perustuu yksityiskohtaisiin ohjeisiin. (Kimbrough & Componation 2009, 21)

Leech (2000, 67–68) on myös puhunut osallistuvan kulttuurin puolesta ja sen merkityksestä jatkuvaan parantamiseen. Leech on esittänyt riskienhallinnan jakoa perinteiseen ja uuteen näkemykseen. Perinteisen näkemyksen mukaan johdon tehtävä on osoittaa tehtävät alaisilleen sekä valvoa heitä, työntekijöiden osallistuminen on rajallista ja toimintaa ohjaavat organisaation politiikat ja säännöt. Sen sijaan uuden näkemyksen mukaan työntekijät tulee valtuuttaa toimimaan itsenäisemmin, mikä tukee osallistuvaa toimintaa ja jatkuvan parantamisen kulttuuria. Leechin tavoin Lam (2003, 22) on esittänyt riskienhallinnan kaksi puolta: kova ja pehmeä. Riskienhallinnan kovalla puolella tarkoitetaan tässä riskivalvontakomiteoita, politiikkoja ja menettelytapoja sekä valvontaprosesseja. Pehmeällä puolella puolestaan viitataan riskitietoisuuteen, luottamukseen ja kommunikaatioon. Leech (2000) puhuu vahvasti uuden näkemyksen puolesta riskienhallinnan toteuttamisessa, kun taas Lam (2003) kannattaa tasapainoa kovan ja pehmeän puolen välillä.

Organisaatiokulttuurin lisäksi kirjallisuudessa puhutaan riskikulttuurista, jossa nimensä mukaisesti korostuu tapa, jolla riskeihin suhtaudutaan. Organisaatiokulttuuri pitää riskikulttuurin sisällään, mikäli organisaatio on niin sanotusti riskiälykäs. Riskiälykkäässä organisaatiossa riskienhallintaa ei nähdä projektina, vaan se on osa kulttuuria, tapa työskennellä. (Deloitte & Touche LLP 2006, 2) Riskikulttuurin olennaisin ajatus on, että kaikessa päätöksenteossa huomioidaan sekä päätöksen riski että tuotto-odotus. Riskikulttuuri edellyttää, että organisaatiossa on olemassa muodollinen, koko organisaation laajuinen prosessi, jolla riskejä hallitaan. Lisäksi jokaisella liiketoimintayksiköllä tulee olla käsitys omasta riskiprofiilistaan. Riskikulttuurin luominen organisaatioon vaatii myös suoritusmittareiden sopeuttamista uuteen kulttuuriin. Suoritusmittareiden muuttaminen on tärkeää, jotta mitataan oikeita asioita, mutta myös siksi, että sillä tuetaan henkilöstön sitoutumista uuteen kulttuuriin sekä lisätään ymmärrystä riskien vaikutuksesta päätöksentekoon. Riskikulttuurin omaksuminen vaatii usein myös kouluttamista ja riskikulttuuriin sitoutuminen palkitsemista oikeanlaisesta riskikäyttäytymisestä. (Buehler & Pritsch 2003, 6)

Riskiälykkään organisaation voidaan siis sanoa olevan sellainen, jossa vallitsee avoin kulttuuri, toiminta on läpinäkyvää, kommunikointi vapaata ja rutiininomaista ja riskit huomioidaan kaikessa organisaation toiminnassa. Liiallinen organisaatiohierarkia estää vapaan kommunikaation alhaalta ylöspäin sekä eri osastojen ja yksiköiden välillä. Riskienhallinnan tehokkuuden voidaan kuitenkin katsoa kärsivän myös siitä, jos organisaatiossa ei ole millään tavoin järjestelmällisesti organisoitu riskienhallintaa. (Buehler & Pritsch 2003, 6; Kimbrough & Componation 2009, 21; Leech 2000, 67–68; Layton & Fuchs 2007; Roche 2012) Riskienhallinnan avointa kulttuuria ja sen ohjeistamista ja valvontaa ei pidäkään nähdä toisiaan poissulkevina, vaan Lamin (2003) näkemyksen mukaan tulisi pyrkiä näiden kahden tasapainoon.

3.2.2 Riskienhallintapolitiikka ja riskienhallinnan työkalut

Jotta riskienhallinta voisi olla tehokasta, systemaattista ja oikea-aikaista tulee sen toteuttamiseen olla selkeä ohjeistus siitä, mitä riskienhallinnan työllä tarkoitetaan, kenen sitä tulee tehdä ja miten sitä tulee tehdä (IIA 2010, 11; ISO 31000:2009, 7). Ohjeistus hei-

jastaa organisaation riskienhallintafilosofiaa (Shenkir & Walker 2011, 13). Kirjallisuudessa ohjeistusta kutsutaan usein riskienhallintapolitiikaksi. Riskienhallintapolitiikan ohella käytetään myös muita käsitteitä, kuten riskienhallintastrategia ja riskienhallinnan periaatteet. Toisinaan käsitteillä viitataan samaan asiaan ja toisinaan ne kuvaavat eritasoisia riskienhallinnan ohjeistuksia.

Riskienhallintapolitiikka linjaa ja määrittelee organisaatiossa harjoitettavaa riskienhallintaa. Se on yleensä hallituksen hyväksymä periaatedokumentti, jonka tulisi olla osa organisaation kokonaisohjausta. Riskienhallintapolitiikan on tarkoitus tukea strategian toteutumista ja siten sen tuleekin olla linjassa organisaation vision, toiminta-ajatuksen ja arvojen kanssa. Politiikka määrittelee yleensä keskeiset riskienhallinnan päämäärät ja tavoitteet, riskienhallinnan organisoinnin ja vastuut sekä sen, mitä riskillä tarkoitetaan. Riskienhallintapolitiikassa voidaan lisäksi määritellä raportointiperiaatteet. Organisaation riskiympäristö on jatkuvan muutoksen alla, joten riskienhallintapolitiikkaa tulee arvioida säännöllisesti ja sitä tulee tarvittaessa mukauttaa organisaation ympäristöön sopivammaksi. Riskienhallintapolitiikan lisäksi yleensä muotoillaan myös toiminnallisemmat periaatteet siitä, mitä riskienhallinnalla tavoitellaan sekä kuvaus riskienhallinnan strategioista ja prosesseista. Lisäksi periaatteissa tulisi raportoida organisaation merkittävimmistä riskialueista sekä riskienhallinnan onnistumisen mittaamisesta. (AIRMIC, ALARM, IRM 2002, 12; Kupi, Keränen & Lanne 2009, 18; Leino, Steiner &Wahlroos 2005, 128–129)

Riskienhallintapolitiikan oheen voidaan muotoilla myös erillinen riskistrategia. Riskistrategialla tarkoitetaan strategiaa, joka kuvaa, mitä mahdollisuuksia organisaatiossa halutaan hyödyntää, mitä riskejä halutaan välttää ja kuinka paljon riskiä ollaan valmiita ottamaan sekä, kuinka paljon tuottoa halutaan riskillä saavuttaa. (Buehler & Pritsch 2003, 43) Yritykset pyrkivät arvon kasvattamiseen, mihin liittyy aina riskejä. Organisaation tuleekin aina arvioida riskin määrää saatavaan hyötyyn verrattuna. Kaikkiin mahdollisuuksiin ei ehkä kyetä tarttumaan riskinottohalun ja -kyvyn rajoittaessa riskinottoa. Organisaation pääoma, teknologia ja henkilöstön kyvyt ovat avainasemassa määriteltäessä, kuinka paljon organisaatio kykenee riskiä kantamaan. Koska organisaation riskinottohalu määrittelee hyvin paljon sitä, millaiseksi riskienhallinta lopulta muodostuu, tulee siitä päättää riskienhallintapolitiikan muotoilun yhteydessä. (Shenkir & Walker 2011, 13)

Käytännön riskienhallinnan tasolla usein tarvitaan riskienhallintapolitiikkaa yksityiskohtaisempaa ohjeistusta siitä, miten riskienhallintaa tulisi tehdä; työkaluja ja tekniikoita, joilla riskienhallintatyön käytäntö sekä helpottuu että yhtenäistyy organisaation eri yksiköiden ja osastojen välillä. Riskienhallintapolitiikka ja -periaatteet jalkautetaankin organisaation erillisten vastuualueille ja -henkilöille suunnattujen ohjeiden avulla. Kuten tutkimuksen toisessa pääluvussa esitettiin riskienhallinnan toteuttamiseen tulisi olla olemassa systemaattinen prosessi, joka ohjaa organisaation henkilöstöä riskien tunnistamisessa, analysoimisessa, riskienhallintatoimenpiteiden valinnassa sekä riskienhallinnan ja riskien seurannassa. (Deloitte & Touche LLP 2006, 8; Leino, Steiner & Wahlroos 2005, 129; Shenkir & Walker 2011, 14–19)

Jotta tehokasta riskienhallintaa varten tehdyistä politiikoista, periaatteista ja käytännön työkaluista olisi todellista hyötyä, tulee niiden olemassaolosta myös viestiä organisaatiossa. Riskienhallintapolitiikan julkaiseminen on yksi keino viestiä riskienhallinnan merkityksestä ja arvostuksesta yrityksessä. (Kupi, Keränen & Lanne 2009, 20) Kun riskienhallintapolitiikka on ymmärretty ja hyväksytty organisaatiossa, on organisaatiolla kaikki mahdollisuudet tehokkaaseen riskienhallintaan (COSO 2004, 28).

Riskienhallintapolitiikan tarkoituksena on siis vaikuttaa siihen, miten organisaatiossa toimitaan. Ei voida kuitenkaan kieltää sitä, etteikö organisaation henkilöstö myös vaikuttaisi siihen, millaiseksi riskienhallinta lopulta muodostuu. Jokaisella organisaation jäsenellä on oma ainutlaatuinen tausta, kyvyt ja prioriteetit, jotka vaikuttavat siihen, kuinka he tunnistavat, arvioivat ja vastaavat riskeihin. Riskienhallinnan vastuiden kohdistamisella sekä vastuukohtaisilla ohjeistuksilla on kuitenkin mahdollista lievittää tätä ilmiötä. (COSO 2004, 18)

3.2.3 Riskiarkkitehtuuri

Riskiarkkitehtuurilla tarkoitetaan tässä niitä rooleja ja vastuita, joita riskienhallintaan liittyy, sekä kommunikointia ja raportointia, jolle riskienhallinta rakentuu.

Jotta riskienhallinnan potentiaali päästäisiin kokonaisuudessaan realisoimaan organisaatiossa, edellyttää se kaikkien organisaation jäsenten sitoutumista riskienhallinnan politiikkaan ja toimintamalleihin. Vaikka riskienhallinnan organisoiminen aloitetaankin usein organisaation ylätasolta muuttamalla hallituksen asenteita ja sitouttamalla johtoa, on tavoitteena kuitenkin riskikulttuurin jalkauttaminen koko organisaatioon siten, että riskienhallinnasta tulee osa organisaation kaikkea toimintaa ja jokaisella organisaation jäsenellä on oma paikkansa riskienhallinnan järjestelmässä. Tavoitteen toteuttamisen kannalta riskienhallinnan viestiminen on merkittävässä asemassa. (AON 2007, 22–23; Cooper, Speh & Downey 2012, 1) Riskienhallinnan tehokas toteuttaminen edellyttää paitsi yhteistä näkemystä riskeistä ja riskienhallinnan tavoitteista, myös selkeää riskienhallinnan roolijakoa (Schild 2009, 55). Siinä missä riskienhallinnan ymmärrystä ja osaamista voidaan lisätä tiedottamisella ja kommunikoinnilla, voidaan organisaation henkilöstöä sitouttaa riskienhallintapolitiikan mukaiseen toimintaan riskienhallinnan vastuiden sisällyttämisellä työnkuvauksiin ja palkkio-ohjelmiin (Cooper, Speh & Downey 2012, 1).

Riskienhallinnan vastuiden yksityiskohtainen määrittely edellyttää systemaattista riskikartoitusta. Kunkin yksikön ja osaston tulisi seurata riskejä, jotka luonnollisesti kuuluvat sen vastuulle. Riskienhallinta voidaan organisoida keskitetysti tai hajautetusti. Riskin luonne ja sen merkitys organisaatiolle sekä johdon halu olla mukana riskienhallinnassa organisaation eri tasoilla vaikuttavat siihen, kumpi tapa valitaan. Keskitetyssä riskienhallinnassa vastuu riskienhallinnasta on yhdellä riskienhallinnasta vastaavalla henkilöllä tai osastolla. Riskienhallinnasta voi vastata myös ylin johto. Keskitetty riskienhallinta toimii yleensä silloin, kun riskit ovat koko organisaatiota koskevia ja sen tavoitteiden ja strategioiden kannalta merkittäviä. Hajautetussa riskienhallinnassa vastuuta jaetaan henkilöille, jotka ovat päivittäin tekemisissä riskien kanssa. (Blumme ym. 2005, 83; Chapman 2001, 32)

Ylin vastuu riskienhallinnan toteuttamisesta on kuitenkin toimitusjohtajalla. Muiden johtajien vastuulla on tukea organisaation riskienhallintafilosofiaa, kannustaa riskinottohalukkuudessa pitäytymiseen ja hallita riskejä omilla vastuualueillaan riskinottohalun rajoissa. Hallituksen tehtävänä on valvoa riskienhallintaa ja varmistua sen toteuttamisesta. Riskienhallinnasta ovat siis vastuussa ennen kaikkea organisaation johto ja hallitus. (COSO 2004, 8; Shenkir & Walker 2011, 12)

Hallitus

Hallituksen tehtävänä on varmistaa, että johto ylläpitää tehokasta riskienhallintaa organisaatiossa. Hallitus paitsi valvoo, se myös ohjaa ja johtaa riskienhallintaan liittyvää toimintaa. Hallituksen vastuulla on muun muassa riskienhallintapolitiikan kehittäminen. (Ingley & Van Der Walt 2008, 44) Hallitus kantaa lopullisen vastuun riskienhallinnasta (AIRMIC, ALARM & IRM 2010, 11). Koska hallituksen pitää olla valmis ja kyvykäs kyseenalaistamaan ja tutkimaan johdon toimia sekä esittämään vaihtoehtoisia näkemyksiä, pitää hallituksessa ensinnäkin olla riittävästi johtamistaitoa, teknistä osaamista sekä muuta asiantuntemusta ja toiseksi hallituksessa tulisi olla myös organisaation ulkopuolisia jäseniä. COSO:n (2004, 29) suosituksen mukaan itsenäisiä, ulkopuolisia jäseniä tulisi olla vähintään enemmistö. Hallituksen tulee olla roolissaan kriittinen, sillä jokainen organisaatio on riskille altis ja tehokasta riskienhallinnan järjestelmän valvontaa tarvitaan kaikissa organisaatioissa. Lisäksi hallituksen sitoutumista riskienhallintaan pidetään organisaation sisäisistä tekijöistä tärkeimpänä kannustimena riskienhallinnan järjestämiseen. (COSO 2004, 29, 83–84; Economist Intelligence Unit 2007, 6, 8; Holopainen ym. 2006, 34; Leino, Steiner & Wahlroos 2005, 130; Shenkir & Walker 2011, 12)

Hallituksen tietokanavana toimii organisaation johto, joka on tilivelvollinen hallitukselle ja, jolta se saa tarvittavat tiedot organisaation riskienhallinnan tilasta. Hallituksen pitää olla selvillä tärkeimmistä riskeistä, johdon toimista sekä siitä, kuinka johto varmistaa riskienhallinnan tehokkuuden. (COSO 2004, 8–9, 83–84; Ingley & Van Der Walt 2008, 49) Käytännössä hallitus usein käyttää varmistustehtävässään apuna lisävoimia. Kuten edellä todettiin sisäinen tarkastus toimii usein riskienhallinnan arvioitsijana. Sisäinen tarkastus antaakin merkittävää lisävarmistusta riskienhallinnan toimivuudesta hallitukselle. Mikäli organisaatio on liian pieni täysaikaisen sisäisen tarkastajan palkkaamiseksi tai jos jostain muusta syystä yrityksessä ei ole sisäistä tarkastusta, voi johto hyödyntää arvioinneissa myös ulkopuolisia tarkastajia. (COSO 2004, 8; Holopainen ym. 2006, 34, 66) Tulee kuitenkin huomata, että riskienhallinnan arviointitehtävän hoitaminen vaatii usein hyvinkin kattavaa organisaation ja sen ympäristön sekä prosessien tuntemista.

Johto

Riskienhallinta on yksi organisaation johtamisen perustehtävistä. Johdon tehtävänä onkin ohjata yrityksen toimintaa siten, että liialliset riskit vältetään, mahdollisuudet käytetään hyväksi ja tavoitteet saavutetaan. Johdon tehtävänä on paitsi tarjota riskienhallinnan visio, tavoitteet ja strategia niin myös käyttäytymisen mallit. (Drew & Kendrick 2005, 28; Holopainen ym 2006, 34) Organisaation johto voi valinnoillaan sekä luoda, että säilyttää arvoa, mutta myös kuluttaa. Jotta toiminta keskittyisi kahteen ensimmäiseen, tulee johdon huomioida sekä organisaation sisäinen että ulkoinen ympäristö, kohdistaa resurssit järkevästi sekä reagoida muuttuviin olosuhteisiin. (COSO 2004, 14)

Johdon vastuut riskienhallinnasta ovat erilaiset eri organisaatiotasoilla. Vastuut voivat vaihdella huomattavastikin organisaation ominaispiirteistä riippuen. Kaikissa yrityksissä toimitusjohtajalla on kuitenkin suurin vastuu riskienhallinnan toteuttamisesta. (COSO 2004, 84) Toimitusjohtajan ja ylimmän johdon vastuulla on suunnitella riskienhallinnan järjestelmä, määritellä riskinottokyky ja toteuttaa riskienhallintaa käytännössä sekä raportoida hallitukselle juoksevasti. Raportointi hallitukselle voi tapahtua esimerkiksi johdon kuukausiraportoinnin yhteydessä. Liiketoimintajohdon vastuulla on päättää toimenpiteistä, jotka ovat linjassa riskienhallinnan odotusten kanssa sekä seurata toteutumia ja verrata niitä odotuksiin. Liiketoimintayksiköiden johdon vastuulla on johtaa omien yksiköidensä riskejä. He vastaavat toteuttamisen organisoinnista ja henkilöstön sitouttamisesta sekä lisäksi he raportoivat säännöllisesti organisaatiossa ylöspäin oman liiketoimintayksikkönsä riskeistä ja niiden hallinnasta. (Cooper, Speh & Downey 2012, 1; COSO 2004, 85; Holopainen ym. 2006, 34; Leino, Steiner & Wahlroos 2005, 130)

Johto on merkittävässä roolissa riskienhallintaa tukevan organisaatiokulttuurin luomisessa. Riskienhallinnan tärkeyden ymmärtäminen ja tunnustaminen organisaation ylemmillä tasoilla vaikuttaa koko muun organisaation suhtautumiseen riskienhallintaan. (Buehler & Pritsch 2003; Shenkir & Walker 2011, 12) Johdon sitoutumattomuus riskienhallintaan ilmenee muun muassa riskienhallintaan uhrattujen resurssien ja ajan puutteina ja johtaa yleensä siihen, että riskienhallinnan toteuttaminen ei onnistu. (Miccolis 2003). Riskinottamiselta ei voida välttyä liiketoiminnassa, mutta ne organisaatiot, jotka ottavat ’oikeita’ riskejä, menestyvät paremmin kuin kilpailijansa. Johdon tulisikin

sekä luoda riskienhallintakulttuuri, jossa riskejä otetaan loogisin perustein että asettaa selkeät linjat hyväksyttävästä riskinoton tasosta. (Psica 2007, 77)

Riskienhallintapäällikkö

Organisaation koosta riippuen riskienhallinnan toimintaa ohjaamaan voi olla nimitetty riskienhallintapäällikkö. Toisinaan riskienhallintaa varten saattaa organisaatiossa olla kokonainen riskienhallintayksikkö, joka vastaa organisaation riskienhallinnan toteuttamisesta yhdessä johdon kanssa. Riskienhallintapäällikön tehtäväkenttä on voitu myös yhdistää jonkin toisen alueen päällikön tehtäväkenttään, esimerkiksi talouspäällikön alle. Organisaation koko yleensä vaikuttaa siihen, kuinka paljon resursseja riskienhallintaan laitetaan. (AIRMIC, ALARM & IRM 2002, 13; COSO 2004, 86)

Organisaation koko vaikuttaa yleensä myös siihen, millaiseksi riskienhallinnan ammattilaisten tehtäväkenttä muodostuu. Pienissä organisaatioissa työ on usein paljon käytännönläheisempää kuin suurissa organisaatioissa. (Holmquist 2011) Riskienhallinnan ammattilaisten vastuulla voivat olla muun muassa seuraavanlaiset tehtävät:

- riskienhallintapolitiikan määrittely;
- riskikulttuurin edistäminen;
- liiketoimintayksiköiden riskirakenteiden luominen;
- henkilöstön kouluttaminen;
- operatiivisen johdon avustaminen riskienhallinnan prosessin toteuttamisessa;
- organisaation riskinkantokyvyn ja riskinottohalun analysoimisessa ja määrittämisessä avustaminen;
- riskien vaikutusten ja todennäköisyyksien laskennassa avustaminen;
- johdon konsultointi;
- riskienhallinnan tehokkuuden mittareiden kehittäminen;
- riskienhallinnan raportointi ja raportoinnin kehittäminen;
- riskienhallinnan toimenpiteiden kustannus-hyöty -tarkasteluiden toteuttaminen (AIRMIC, ALARM & IRM 2002, 13; Shenkir & Walker 2011, 7).

Riskienhallintaa ei tulisi kuitenkaan koskaan nähdä täysin erillisenä vastuualueena, vaan riskienhallinta on luonnollinen osa jokaisen toiminnan menestymisestä vastaavan johtajan työtä (Veijola 2012, 49). Riskienhallinnan ammattilaisten tulisikin työskennellä yhteistyössä johdon kanssa. Riskienhallintapäällikkö tai -yksikkö voi raportoida työstään

joko toimitusjohtajalle tai suoraan hallitukselle, mikä lisää sen riippumattomuutta organisaatiossa. (COSO 2004, 87; Shenkir & Walker 2011, 6) Raportoidessaan hallitukselle on riskienhallinnan ammattilaisten rooli ja tehtäväkenttä yleensä hieman erilainen keskittyen enemmän riskienhallinnan tilan arviointiin ja muutosehdotusten tekemiseen. Seurannan ja raportoinnin rooli korostuvat tällöin heidän työssään ja tehtäväkenttä muistuttaakin paljon sisäisen tarkastuksen tehtäväkenttää. (COSO 2004, 86; Holopainen ym. 2006, 15, 36, 66)

Työntekijät

Johtaminen ei ole enää vain johtajien ja esimiesten yksinoikeus tai velvollisuus, vaan organisaation on menestyäkseen otettava koko henkilöstö mukaan vaikuttamaan siihen, miten asioita tehdään (Kauppinen 2002, 22). Organisaatioiden riskitekijöiden määrä voi olla niin suuri ettei johto ja hallitus kykene niitä kaikkia tutkimaan ja valvomaan, joten niistä huolehtiminen on siirrettävä alemmille organisaatiotasoille. Tarkoituksena ei kuitenkaan ole vain helpottaa oikea-aikaista riskienhallintaa, vaan myös kannustaa vastuullisuuteen riskienhallinnan osalta. (Wood 2005, 27) Käytännöllisesti katsoen kaikki työntekijät ovat jonkinlaisessa riskienhallinnan roolissa. He voivat esimerkiksi tuottaa tietoa, jota käytetään hyväksi riskien tunnistamisessa tai niiden arvioinnissa. Huolellisuus, jolla organisaatiossa toimitaan vaikuttaakin siis suoraan riskienhallinnan tehokkuuteen. Olennaista on myös se, että organisaatiossa riskeihin liittyvä tieto virtaa vapaasti työntekijöiden ja johdon välillä. (COSO 2004, 88)

Organisaatiokulttuurin tulisi tukea riskienhallinnan tavoitteiden ymmärtämistä ja niiden saavuttamista läpi organisaation. Pelkästään hallituksen ja ylimmän johdon ymmärrys ja tuki eivät riitä. Erityisesti keskijohto, joka toimii työntekijärajapinnassa on merkittävässä asemassa riskienhallinnasta tiedotettaessa. Mikäli työntekijät eivät ole tietoisia omasta riskienhallintaroolistaan eivätkä organisaation riskienhallintapolitiikasta, eivät he voi toiminnallaan myöskään tukea riskienhallintaa. Lopputuloksena on, että organisaatiossa ei koskaan päästä realisoimaan riskienhallinnan koko potentiaalia. (AON 2007, 22) Riskienhallinta onkin osa kaikkien organisaation henkilöiden työtehtäviä tavalla tai toisella, joten henkilöiden roolit sekä vastuut tulisi määritellä riittävän tarkasti sekä viestiä tehokkaasti (COSO 2004, 89; Economist Intelligence Unit 2007, 2).

Sisäinen viestintä

Sisäisellä viestinnällä tarkoitetaan organisaation sisäistä tiedonkulkua ja vuorovaikutusta, jonka tarkoituksena voi olla esimerkiksi toiminnan ydinprosessien tukeminen, sitoutumisen lisääminen ja muutosprosessien tukeminen. Ydinprosessien tukemisella tarkoitetaan tiedonvaihtoa, jota edellytetään organisaation perustehtävän toteuttamiseksi mahdollisimman hyvin. Sitoutuminen organisaatioon ja sen käytäntöihin on yleensä sitä parempi mitä enemmän organisaatiossa tunnetaan sen toimintaa, strategiaa ja perustehtäviä. Erityisesti muutostilanteissa sisäinen viestintä on merkittävässä roolissa. Muutosten läpivienti edellyttää organisaation ymmärrystä muutoksen merkityksestä ja sen edellytyksistä. (Vos & Schoemaker 2005, 78–79) Viestinnällä tarkoitetaan tutkimuksessa myös sitä raportointia, joka liittyy riskienhallintaa. Organisaatiossa voidaan toimia sitä tehokkaammin mitä parempaa viestintä on. Viestinnän tulisikin olla oikea-aikaista, ymmärrettävää, virheetöntä, asianmukaista ja uskottavaa. (Marques 2010, 51)

Viestintä on osa kaikkia riskienhallintaprosessin vaiheita (ISO 31000:2009, 14). COSO:n esittämässä viitekehyksessä (2004, 23) ”tieto ja viestintä” muodostavatkin yhden kahdeksasta kokonaisvaltaisen riskienhallinnan komponentista. Johdon vastuulla on kehittää ja toteuttaa organisaatiossa sellainen viestintäjärjestelmä, jonka avulla voidaan ilmaista organisaation riskikäsitys sekä riskienhallintasuunnitelmat. Viestintäkanavien tulee toimia kuitenkin myös toiseen suuntaan: työntekijöiltä johdolle. (Frigo & Anderson 2009, 33) Tällainen kaksisuuntainen viestintä vaatii johdolta kuuntelemista, lähellä olemista ja avoimuutta (Grunig 1992, 231). Lisäksi hallitus tarvitsee työssään riskienhallinnan tietoa, jonka avulla se pystyy toteuttamaan valvontavastuunsa. Samalla tavoin hallituksen tulisi viestiä sen tietotarpeista johdolle sekä antaa palautetta ja ohjausta. (COSO 2004, 67–68; Shenkir & Walker 2007, 25)

Tietoa, joka liittyy organisaation avainriskeihin tulisi jakaa koko organisaatiossa. Kuten edellä on todettu, kaikki organisaation jäsenet tavalla tai toisella osallistuvat riskienhallinnan toteuttamiseen, joten kaikilla organisaatiotasoilla pitäisi olla riittävästi tietoa riskeistä ja riskienhallinnan toimintatavoista. (Frigo & Anderson 2009, 33) Riskienhallinnan viestintä on tärkeää, koska päätöksentekijöiden omat käsitykset riskeistä vaikuttavat merkittävästi siihen, miten he riskeihin reagoivat. Nämä käsitykset voivat vaihdella arvojen, tarpeiden, oletusten ja ajatusten mukaan. Viestinnällä voidaan vaikuttaa päätök-

sentekijöiden käsityksiin ja heidän tekemiinsä päätöksiin. Nämä erilaiset taustat ja arvot tulisikin tunnistaa organisaatiossa, jotta niihin voitaisiin viestinnällä vaikuttaa. (ISO 31000:2009, 14–15)

Riskienhallinnan kannalta on oleellista, että viestintä tapahtuu roolien, tiimien ja organisaatioiden yksiköiden rajapinnoissa (Kauppinen 2002, 23–24). Merkittävä tieto siirtyy näin organisaatiossa sekä vertikaalisesti että horisontaalisesti, mikä mahdollistaa muun muassa organisaation erilaisten asiantuntijoiden ajatusten vaihdon. Viestinnän avulla siis paitsi siirretään merkittävää tietoa, mahdollistetaan myös organisaation eri yksiköiden yhdessä oppiminen ja kehittyminen. (COSO 2004, 22; ISO 31000:2009, 14; Frigo & Aanderson 2009, 33; Shenkir & Walker 2011, 20)

3.2.4 Riskin juurruttaminen prosesseihin ja päätöksentekoon

Riskit ovat luonnollinen osa organisaatioiden tavoitteellista toimintaa. Riskienhallinnalla ei pyritäkään riskivastaisuuteen, vaan sen tarkoituksena on avustaa organisaatiota toimimaan ennakoivasti ja riskiperusteisia päätöksiä tehden, jolloin riskinotto on tietoista ja perusteltua. (Shenkir & Walker 2011, 20) Perinteisestä riskienhallinnasta kokonaisvaltaiseen riskienhallintaan siirtymisellä tarkoitetaan muun muassa siirtymistä päätöksenteon seurausten hallinnasta riskitietoiseen päätöksentekoon. Tavoitteena on siis parantaa päätöksentekijöiden varmuutta selkeämmän riskikäsityksen avulla, vaikka päätösten seurausten hallinta on myös edelleen osa riskienhallintaa. (Shenkir & Walker 2007, 24–25; Shortreed 2010, 10)

Päätöksentekotilanteisiin liittyy lähes aina epävarmuutta ja riskille altistumista, mistä johtuukin, että riskienhallinnan tulisi olla luonnollinen osa päätöksentekoa (Buehler, Freeman & Hulme 2008, 103). Nottinghamin (1997, 27) mukaan riskienhallinnan päätarkoitus onkin auttaa juuri päätöksenteossa. Layton ja Fuchs (2007) ovat todenneet, että riskiälykkään organisaation muodostaminen edellyttää, että riskienhallinta liitetään osaksi päätöksentekoprosessia. Riskienhallinta ei siis voi olla tehokasta jos se on vain tarkistuslista tai prosessi, joka on erillään liiketoiminnan päätöksenteosta (PwC 2008, 12). Riskien analysointi tuo uuden näkökulman liiketoiminnan päätöksentekoprosesseihin sekä välineitä vaihtoehtoisten päätösten tekemiseen (Kyrölä 2010, 62). Kun päätökset tehdään saatavilla olevan parhaan tiedon pohjalta, eri näkökulmat huomioiden, ovat

päätökset usein harkitumpia (ISO 31000:2009, 7).

Päätöksentekijöiden tulisi analysoida päätösten vaikutuksia organisaation kokonaisriskin kannalta ja tehdä kompromisseja siten, että riskinotto pysyisi organisaation kannalta järkevänä. Hyvä riskienhallinta yleensä edellyttääkin, että riskienhallintaa ohjataan kaikilla organisaatiotasoilla ja kannustetaan riskinottoon, jossa huomioidaan koko organisaation pitkän tähtäimen tavoitteet. (Buehler, Freeman & Hulme 2008, 108)

Jotta riskienhallinta onnistuttaisiin liittämään onnistuneesti osaksi organisaation päätöksentekoa, tulee riskienhallinnan käytännöt liittää organisaation prosesseihin. Tämä puolestaan edellyttää, että organisaatio sekä tunnistaa että tuntee prosessinsa ja toimintonsa riittävän syvällisesti. Prosessikuvaukset voivat auttaa organisaatiota hahmottamaan toimintansa kokonaiskuvan paremmin ja sen avulla on myös helpompi kerätä toimintaan liittyvää riskitietoa. (Kupi, Keränen & Lanne 2009, 12, 40) Kai Laamasen (2005, 19) määritelmän mukaan liiketoimintaprosessi on joukko loogisesti toisiinsa liittyviä toimintoja ja niiden toteuttamiseen tarvittavia resursseja, joiden avulla saadaan aikaan toiminnan tulokset. Kun riskienhallinta liitetään osaksi prosesseja, voidaan organisaatiossa paremmin tunnistaa riskejä juuri sillä organisaatiotasolla, jossa ne syntyvätkin (COSO 2004, 17–18; Psica 2007, 77). Riskitarkasteluiden sisällyttäminen liiketoiminnan prosesseihin ja käytäntöihin varmistaa myös osaltaan, että organisaatiossa toimitaan riskinottohalun ja -kyvyn rajoissa (PwC 2008, 12).

Kun riskienhallinta on systemaattinen kokonaisuus, joka perustuu ennalta muotoiltuun politiikkaan ja strategiaan, on riskienhallinnan liittäminen prosesseihin sujuvampaa. Riskistrategia vaikuttaa kaikkeen päätöksentekoon organisaatiossa. Hyvästä strategiasta käy ilmi, mitä riskejä organisaatiossa halutaan ottaa sekä riskin määrä, jonka organisaatio pystyy kantamaan sekä tuotot, joita se edellyttää saavansa riskinotosta. Näiden suuntaviivojen avulla liiketoimintayksiköiden johdon on helpompi sopeuttaa omaa toimintaansa organisaation tavoitteiden mukaiseksi. (Buehler & Pritsch 2003, 5) Riskienhallinnan liittäminen osaksi prosesseja ja päätöksentekoa vaatii lisäksi riskienhallinnan vastuiden selkeää roolijakoa, johdon sitoutumista ja mahdollisesti myös lisäkoulutusta riskienhallinnan viitekehyksestä ja toteuttamisesta. (Buehler, Freeman & Hulme 2008, 109)

3.2.5 Riskit osa johtamisjärjestelmää

Johtamisjärjestelmällä tarkoitetaan strategista ja operatiivista suunnittelua, tavoitteiden asettamista ja seurantaa sekä strategian toimivuudesta oppimista. Johtamisjärjestelmällä tarkoitetaan myös kaikkea sitä systemaattista toimintaa, jolla organisaation johto pyrkii varmistamaan sen menestymisen. (Malmi, Peltola & Toivanen 2006, 38) Organisaation riskienhallintastrategian tulee tukea organisaation perusperiaatteita. Tehokkain tapa varmistaa, että riskienhallinta todella tukee organisaation muuta toimintaan, on yhdistää riskienhallinta osaksi tavanomaista johtamista ja toiminnan prosesseja. Kun riskienhallinta liitetään systemaattiseksi osaksi johtamista, riskienhallinnan fokus laajenee pelkästä vahinkojen välttämisestä asetettujen tavoitteiden saavuttamisen tukemiseen ja näin riskienhallinnasta tulee osa organisaation muuta toimintaa ja johtamista. (Kupi, Keränen, Lanne 2009, 12, 14)

Organisaation toiminta perustuu sen toiminta-ajatukselle, missiolle, jonka pohjalta johto laatii strategiset tavoitteet. Strategiset tavoitteet siis heijastavat sitä, kuinka organisaatio aikoo luoda arvoa sen sidosryhmille. Strategisten tavoitteiden saavuttamiseksi luodaan strategia, josta sitten johdetaan niin sanottuja alatavoitteita, jotka osoitetaan organisaation eri liiketoimintayksiköille, osastoille ja prosesseille. Näihin erilaisiin, vaihtoehtoisiin strategioihin, joilla pyritään saavuttamaan strategiset tavoitteet sisältyy epävarmuutta, jota tulisi pyrkiä parhaalla mahdollisella tavalla ennustamaan. Riskienhallinnan tekniikoita soveltamalla lopulta päätetään, mitä strategiaa organisaatiossa lähdetään toteuttamaan. (COSO 2004, 18–19, 35, 36; Kaplan & Norton 2004, 27; Raynor 2007)

Riskienhallinnan tulisi siis olla strategiakehystä täydentävä, ei erillinen toiminto. Jos strategia muotoillaan siten, että siihen sisältyviä riskejä ei tunnisteta, on strategia epätäydellinen ja riskille alttiimpi. Huono strategisten riskien hallinta onkin osoittautunut yhdeksi merkittävimmistä syistä, miksi organisaation omistaja-arvoa ei kyetä säilyttämään saati kasvattamaan. Organisaation strategiaa muotoiltaessa ylimmän johdon tulee siis analysoida sen strategiset vaihtoehdot ja tunnistaa ne tapahtumat, jotka voivat uhata vaihtoehtoisten strategioiden toteutumista. Kun jokaisen strategiavaihtoehdon riskit on tunnistettu ja sijoitettu riskikarttaan, voidaan vaihtoehtoja arvioida organisaation riskinottohaluun vertaamalla. Riskien huomioiminen strategiasuunnittelussa auttaa johtoa

tekemään harkittuja ja perusteltuja valintoja ja näin riskienhallinta tukee osaltaan järkevää liikkeenjohtamista. (Gibbs & DeLoach 2006, 36; Shenkir & Walker 2011, 20–21)

Mikäli strategiaa ei sopeuteta riskinottohalun mukaiseksi, voi seurauksena olla liian suuren tai liian vähäisen riskin hyväksyminen. Mikäli organisaation tavoitteet edellyttävät X määrän riskinottoa, mutta sen riskinottohalu onkin vain X-1, niin tällöin seurauksena on, että organisaatio joko hyväksyy liian suuren määrän riskiä, jotta se pääsee tavoitteisiinsa tai vaihtoehtoisesti jos se toimii riskinottohalunsa rajoissa, ei se voi saavuttaa tavoitteitaan. Arvoa voidaan maksimoida asettamalla strategia ja tavoitteet siten, että kasvu- ja tuottotavoitteet ovat optimaalisessa tasapainossa riskien kanssa. (COSO 2004, 39; Head 2009, 69; KPMG 2005, 85) Kun riskit huomioidaan jo strategisuunnittelun yhteydessä, on organisaatiolla mahdollisuus löytää tapa luoda arvoa pienemmällä riskillä (Raynor 2007).

Kun tavoitteet on valittu, tulee tarkemmin arvioida sekä strategisia että operatiivisia riskejä ja tehdä tarvittavia toimenpiteitä riskien hallitsemiseksi. Lisäksi uudet esiin tulevat potentiaaliset mahdollisuudet tulee huomioida. Riskienhallinnalla voidaan luoda kohtuullinen varmuus siitä, että strategiset ja operatiiviset tavoitteet saavutetaan. (COSO 2004, 14, 20, 35, 39; Shenkir & Walker 2011, 13; Shenkir & Walker 2007, 1) Sen lisäksi, että riskienhallinta on siis mukana strategian luomisessa, sen avulla voidaan ennakoida ja hallita niitä riskejä, jotka uhkaavat strategian ja tavoitteiden toteutumista (KPMG 2005, 85). Perusteellinen riskien tunnistaminen lähtee liikkeelle strategisten tavoitteiden analysoimisesta ja pääprosessirakenteiden luetteloimisesta, jonka jälkeen pohditaan, mikä voisi mennä pieleen kunkin prosessin osalta. (Schild 2009, 55)

Integroimalla riskienhallinta osaksi organisaation strategiaprosessia voidaan saavuttaa kestävää kilpailuetua, optimoida riskienhallinnan kustannukset sekä auttaa johtoa parantamaan organisaation liiketoimintaa. Riskienhallinta auttaa siis organisaatiota suojelemaan ja kasvattamaan arvoaan. (Gibbs & DeLoach 2006, 36) Toisaalta organisaation strategia ohjaa riskienhallintaa siltä osin, mitä riskejä otetaan ja mitä vältetään. (Kupi, Keränen & Lanne 2009, 11) Strategia on dynaaminen; se muuttuu ympäristön muutosten mukaan. Näin ollen myös riskienhallinnan tulee muuttua ajassa. (Gibbs & DeLoach 2006, 35) Schild (2009, 55) onkin todennut, että riskienhallinta ei voi olla ’täydellistä’ ellei sitä sopeuteta strategisiin tavoitteisiin. Huomioimalla nämä lähtökohdat, luodaan

pohja strategia-riskikeskeiselle organisaatiolle, jolla on suorempi tie arvon tuottamiseen sekä suuremmat mahdollisuudet muiden tavoitteiden saavuttamiseen (COSO 2004, 19; Shenkir & Walker 2011, 21).

Balanced Scorecard

Tasapainotettu mittaristo eli balanced scorecard (BSC) on johtamisen työkalu, jolla pyritään ohjaamaan ihmisten toimintaa organisaatiossa. Tasapainotettu mittaristo toimii yleensä organisaation johtamisjärjestelmän osana ja sillä mitataan organisaation suorituskykyä. Tasapainotettu mittaristo tuloksellisuuden arvioinnin välineenä on kuitenkin sikäli erilainen, että siinä hyödynnetään monipuolista arviointitietoa. Taloudellista tuloslaskentaa ja tasearviointia täydennetään laadullisen ja inhimillisen pääoman kehitystä kuvaavilla mittareilla. (Malmi, Peltola &Toivanen 2006, 38) Arviointimalli luodaan organisaation keskeisimpien menestystekijöiden varaan. Näkökulmat, joista organisaation toimintaa tarkastellaan tulee luoda siten, että organisaation visio ja strategia voidaan ilmaista niiden avulla. Tarkoitus on siis muuttaa organisaation ajatus siitä, miten se aikoo tulevaisuudessa luoda kestävää arvoa, operatiivisiksi käsitteiksi ja niin ikään toiminnaksi. Perinteiset tasapainotetun mittariston näkökulmat ovat: asiakkaat, sisäinen liiketoiminta, innovaatio ja oppiminen sekä talous. Näille ulottuvuuksille laaditaan sitten jokaiselle omat mittarinsa ja suoritustavoitteensa ja aina analyysikauden päätteeksi analysoidaan tiedot. (Kaplan & Norton 2002, 32–43; Kaplan & Norton 2004, 27)

Tasapainotettu mittaristo toimii siis sekä strategisen suunnittelun ja johtamisen että toiminnan kokonaisarvioinnin välineenä. Strategisessa johtamisessa on kysymys organisaation mukauttamisesta strategiaan, eri näkökulmien ja tehtävien yhdistelemisestä sekä tulosten jatkuvasta seurannasta. (Kaplan &Norton 2002, 13; Malmi, Peltola & Toivanen 2006, 21) Organisaation kaikkien tasojen tulisi ymmärtää strategia ja kyetä yhdistämään resurssinsa sen toteuttamiseksi sekä testaamaan strategiaa ja tekemään muutoksia tulosten perusteella (Kaplan & Norton 2002, 14). Tasapainotetun mittariston tehokkuus perustuukin siihen, että sen avulla strategia voidaan ilmaista selkeästi ja strategiasta tulee luonnollisesti osa johtamisjärjestelmää (Kaplan & Norton 2006, 259).

BSC pakottaa johdon määrittelemään täsmällisesti, mitä strategisilla tavoitteilla ja strategialla tarkoitetaan, sillä ne pitää muuttaa mitallisiksi määreiksi, jotta niitä voidaan mi-

tata tasapainotetulla mittaristolla. Tämä edellyttää kommunikointia tavoitteista ja näin voidaankin olettaa, että prosessin tuloksena saavutetaan parempi yhteisymmärrys niin tavoitteista kuin niistä keinoistakin, joilla tavoitteisiin pyritään. (Malmi, Peltola, Toivanen 2006, 19)

Riskienhallinta voidaan yhdistää osaksi tasapainotettua mittaristoa, mikä voi edelleen parantaa sekä riskienhallintaa että organisaation toimintaa ylipäänsä. Riskienhallinta yhdistettynä tasapainotettuun mittaristoon lisää arvoa tunnistamalla ja hallitsemalla niitä tapahtumia, jotka voisivat estää siinä olevien tavoitteiden saavuttamisen ja strategian toteutumisen. Seuraamalla mittareiden tuloksia saadaan tietoa siitä, kuinka tehokkaasti riskienhallinnan keinot ovat toimineet. (Shenkir & Walker 2011, 22) Lisäksi tasapainotetun mittariston kautta voidaan jakaa vastuuta tavoitteista, joten riskienhallinnan liittäminen osaksi mittaristoa johtaisi luonnollisesti siihen, että myös riskienhallinnan vastuukenttä selkenisi (Malmi, Peltola & Toivanen 2006, 20). Lisäksi yhdistämällä riskienhallinta osaksi tasapainotettua mittaristoa, voitaisiin varmistua siitä, että riskienhallinta on sekä strategialähtöistä että siitä muodostuu luonnollinen osa organisaation johtamisjärjestelmää.

Tasapainotetun mittariston rinnalle voitaisiinkin luoda tasapainotettu riskimittaristo, jolla voitaisiin osoittaa riskienhallinnan vastuut BSC:n näkökulmien tunnistetuista avainriskeistä. Näiden kahden mittariston yhteensovittamista on havainnollistettu kuviossa 3. Lähtökohtana on tietyn näkökulman tietyt tavoitteet, joiden avainriskit ja niiden hallitsemiseksi ehdotetut toimenpiteet ovat kortissa seuraavana. Riskiluokalla tarkoitetaan tässä sitä, kuuluuko riski strategisiin, operatiivisiin vai taloudellisiin riskeihin. Riskienhallinta olemassa -sarakkeeseen kirjataan johdon arvio siitä, onko riskiin jollakin tavalla reagoitu. Ja mikäli on, niin kuinka tehokasta se on ollut. Viimeiseen sarakkeeseen merkitään henkilö, joka on vastuussa kyseisestä riskistä. (Shenkir &Walker 2011, 22)

Taloudelliset tavoitteet				**Riskienhallintaprosessi**				
Tavoite	Riskiluku	Riski	Ehdotetut hallintatoi-menpiteet	Riskiluokka	Riskienhallinta olemassa	Tehokkuus	Kommentit	Vastuu-henkilö

Kuvio 3 Balanced Scorecard ja strateginen riskien arviointi (Mukaillen Shenkir & Walker 2011, 22)

Kaikkien mittausjärjestelmien tulisi motivoida niin johtoa kuin muitakin organisaation henkilöitä implementoimaan liiketoimintayksiköiden strategiat onnistuneesti. Ne yritykset, jotka onnistuvat muuttamaan strategiansa mittausjärjestelmäksi, onnistuvat huomattavasti paremmin toimeenpanemaan strategiansa, koska mittausjärjestelmän avulla organisaatio voi konkreettisesti kommunikoida tavoitteensa. Tasapainotettu mittaristo toimiikin tehokkaana strategian viestimisen välineenä. Samalla tavalla sitä voitaisiin soveltaa riskienhallinnan viestimisessä ja organisaation mukauttamisessa riskienhallinnan periaatteiden mukaiseksi sekä riskienhallinnan toimenpiteiden vaikuttavuuden mittaamisessa. (Kaplan & Norton 2002, 235; Kaplan & Norton 1996, 147)

3.2.6 Seuranta, arviointi ja jatkuva parantaminen

Ympäristö, jossa organisaatio toimii, muuttuu jatkuvasti. Riskienhallintakeinot, jotka olivat joskus tehokkaita, voivat seuraavana hetkenä olla täysin epärelevantteja, tai organisaation tavoitteet joudutaan määrittelemään uudelleen. Riskienhallinnan seuranta ja sen tehokkuuden arviointi jatkuvasti muuttuvassa ympäristössä onkin hyvin merkityksellinen riskienhallinprosessin osa. (COSO 2004, 75; IIA 2010, 3–4; ISO 31000:2009, 20) Riskienhallintaprosessin seurannan ja arvioinnin avulla varmistutaan, että prosessi toteutuu joka vaiheessa siten kuin on suunniteltu. Lisäksi riskienhallinnan seurannan avulla saadaan tietoa, jota voidaan hyödyntää riskiarvioinneissa sekä sen avulla organisaatiossa voidaan oppia tapahtumista, muutoksista, onnistumisista ja epäonnistumisista. Arviointien tulisikin olla sekä riskilajikohtaisia että koko riskienhallintaprosessin toimivuutta mittaavia. (Galloway & Funston 2000, 25; Kupi, Keränen & Lanne 2009, 19)

Seurannan ja arviointien perusteella organisaatiossa tehdään tarvittavia muutoksia riskienhallinnan järjestelmään (COSO 2004, 22).

Riskienhallinnan seuranta voidaan toteuttaa joko johdon jatkuvana seurantana, erillisinä arviointeina tai näiden molempien yhdistelmänä. Mitä tehokkaampi jatkuva seuranta organisaatiossa on, sitä vähemmän on tarvetta erillisille arvioinneille. Jatkuva seuranta voi olla tehokkaampaa kuin erilliset arvioinnit, koska sitä tehdään reaaliaikaisesti ja se mahdollistaa dynaamisen toiminnan jatkuvassa muutoksessa. Lisäksi jatkuva seuranta tulisi rakentaa kiinni organisaation muihin toimintoihin, jolloin se juurtuu luonnolliseksi osaksi organisaation normaalia toimintaa. Organisaatio saattaa kuitenkin tehokkaasta jatkuvasta seurannasta huolimatta tehdä erillisiä arviointeja, koska ne ovat yleensä objektiivisempia kuin jatkuva seuranta, joka yleensä perustuu itsearvioinneille. (COSO 2004, 75; IIA 2010, 4) Seuranta edellyttää suoritusmittareiden olemassaoloa. Jatkuva seuranta voidaankin toteuttaa edellä esitetyn tasapainotetun mittariston avulla. (Shenkir & Walker 2011, 22)

Seurannan vastuu on perinteisesti jaettu usealle taholle: johdolle, sisäiselle tarkastukselle ja riskienhallinnan asiantuntijoille. Jotta resurssien käyttö olisi mahdollisimman tehokasta, tulee seurannan työtehtävät koordinoida organisaatiossa. Jos riskienhallinnan seurantaa tehdään useissa erillisissä, itsenäisissä yksiköissä ilman tehokasta koordinointia ja raportointia, saattaa seurannasta tulla päällekkäistä tai avainriskejä voi jäädä huomioimatta. (IIA 2010, 4)

Seurannan tulokset pitää viestiä sekä organisaation sisällä että sen ulkopuolelle asianmukaisella tavalla (ISO 31000:2009, 20). Kaikki havaitut riskienhallinnan puutteet, jotka vaikuttavat organisaation mahdollisuuteen saavuttaa sen tavoitteet, tulisi raportoida erityisesti niille, jotka ovat vastuussa puutteiden korjaamisesta. Puutteiden raportoinnin lisäksi tunnistetut mahdollisuudet, jotka kasvattavat todennäköisyyttä, että yrityksen tavoitteet saavutetaan, tulisi raportoida. (COSO 2004, 80) Jatkuvassa parantamisessa on kysymys riskienhallinnan tavoitteista, mittaamisesta, arvioinneista, prosessin mukauttamisesta sekä käytettävissä olevista resursseista. (ISO 31000:2009, 22) Seurannan tulosten raportoinnilla tuetaankin organisaation oppimista riskeistä sekä tarjotaan puitteet riskienhallinnan jatkuvalle parantamiselle (Chapman 2001, 35).

3.3 Yhteenveto tutkimuksen teoreettisesta viitekehyksestä

Riskienhallintaa on lähestytty edellä sisäisen tarkastuksen työhön kehitettyjen ammattiohjeistusten ja standardien pohjalta. Ohjeistuksissa ja standardeissa annetaan kriteerejä, joilla voidaan arvioida sitä, kuinka toimivaa ja tehokasta riskienhallinta on. Kriteerien mukainen riskienhallintajärjestelmä tarkoittaa seuraavien tekijöiden huomioimista: riskienhallintaprosessin komponentit, riskienhallintaa tukeva organisaatiokulttuuri, toimintaa ohjaava riskienhallintapolitiikka sekä käytännön työtä helpottavat ja systematisoivat riskienhallinnan työkalut, riskienhallinnan roolijako, viestintä, riskiajattelun liittäminen osaksi suunnittelua ja päätöksentekoa sekä seuranta ja jatkuvan parantaminen. Kriteerien mukainen riskienhallinta perustuu kokonaisvaltaisen riskienhallinnan ajatukselle, jossa tavoitteena on hallita riskejä holistisesti osana organisaation muuta toimintaa (Kimbrough & Componation 2009, 19; McShane, Nair & Rustambekov 2011, 644).

Riskienhallintajärjestelmän keskiössä on riskienhallinnan prosessi, joka halutaan sitoa kiinni organisaation muuhun toimintaan. Riskienhallinnan tulisi mallin mukaan olla kiinteä osa organisaation suunnittelu- ja päätöksentekoprosesseja, jotta se tukisi osaltaan organisaation perusperiaatteita. (Kupi, Keränen, Lanne 2009, 12, 14; Shenkir & Walker 2011, 20) Riskien huomioiminen strategia- ja päätösprosessien yhteydessä auttaa johtoa tekemään harkittuja, tietoon perustuvia valintoja, jolloin myös menestymisen mahdollisuudet ovat paremmat, ja organisaatio voi luoda arvoa pienemmällä riskillä (Gibbs & DeLoach 2006, 36; Raynor 2007; Shenkir & Walker 2011, 20–21; Shortreed 2010, 10). Riskitarkasteluiden sisällyttämisellä suunnitteluun ja päätöksentekoon varmistetaan lisäksi, että organisaatiossa toimitaan riskinkantokyvyn rajoissa (PwC 2008, 12).

Riskienhallinnan juurruttaminen organisaation muuhun toimintaan edellyttää, että organisaatiokulttuuri on riskiajattelua tukeva (Miccolis 2003). Kun riskienhallintaa varten on lisäksi kehitetty systemaattinen prosessi, joka perustuu politiikkoihin ja ohjeistuksiin, jotka on viestitty organisaatiossa, on riskienhallinnan liittäminen osaksi suunnittelu- ja päätöksentekoprosesseja helpompaa (Buehler & Pritsch 2003, 5). Integraatio vaatii myös riskienhallinnan vastuiden selkeää roolijakoa, johdon sitoutumista ja mahdollisesti myös lisäkoulutusta riskienhallinnan viitekehyksestä ja toteuttamisesta (Buehler, Freeman & Hulme 2008, 109).

Riskienhallinnan seuranta ja arviointi ovat riskienhallinnan tehokkuuden kannalta oleellisessa roolissa (IIA 2010, 3–4). Riskienhallinnan seurannan avulla varmistutaan, että se toimii joka vaiheessa siten kuin on suunniteltu ja toisaalta jos siinä ilmenee poikkeamia suunniteltuun, voidaan riskienhallintaan tehdä muutoksia tarvittaessa (COSO 2004, 22; Galloway & Funston 2000, 25). Riskienhallinnan arvioinnissa voidaan hyödyntää tasapainotettua mittaristoa, jonka avulla voidaan siis tarkastella, kuinka tehokkaasti riskienhallinnan keinot ovat toimineet (Shenkir & Walker 2011, 22). Lisäksi riskienhallinnan liittäminen tasapainotettuun mittaristoon tukee riskienhallinnan tavoitteiden viestimistä (Kaplan & Norton 2002, 235).

Organisaatiolla tulee olla kokonaiskuva siitä, miltä sen täydellinen riskienhallinnan järjestelmä näyttää, jotta se voi koota kaikki järjestelmän palaset yhteen ja muodostaa niistä tehokkaan järjestelmän osaksi organisaation muuta toimintaa. Seuraavissa luvuissa riskienhallinnan järjestelmää tarkastellaan kohdeyrityksen kannalta tarkemmin.

4 EMPIIRINEN AINEISTO JA RISKIENHALLINNAN NYKYTILA

4.1 Case: Pirkanmaan Osuuskauppa

Pirkanmaan Osuuskauppa (POK) kuuluu S-ryhmään. S-ryhmä on yritysverkosto, joka koostuu Suomen Osuuskauppojen Keskuskunnasta (SOK) ja sen tytäryhtiöistä sekä 20 alueosuuskaupasta ja 8 paikallisosuuskaupasta. Osuuskaupat ovat osuustoiminnallisia yrityksiä. Pirkanmaan Osuuskauppa on yksi 20:sta alueosuuskaupasta ja toimii nimensä mukaisesti Pirkanmaan alueella. (S-kanava: osuuskaupat) Pirkanmaan Osuuskaupalla oli vuoden 2011 lopussa päivittäis- ja käyttötavarakaupan yksiköitä yhteensä 56 ja ravintoloita 14. Näiden lisäksi Pirkanmaan Osuuskaupalla oli seitsemän liikennemyymälää ja 19 automaattiasemaa. Pirkanmaan Osuuskaupan liikevaihto vuonna 2011 oli noin 724, 9 miljoonaa euroa, joka oli 9,5 prosenttia kasvua edelliseen vuoteen verrattuna. Pirkanmaan Osuuskauppa työllisti lähes 3 000 henkilöä vuonna 2011. (Pirkanmaan Osuuskaupan vuosikertomus 2011)

Pirkanmaan Osuuskauppa on itsenäinen osuustoiminnallinen yritys, jonka omistajia ovat sen jäsenet, joita kutsutaan S-ryhmässä asiakasomistajiksi. Kukin asiakasomistaja on sijoittanut osuuskaupan pääomaan samansuuruisen, osuuskaupan säännöissä määritellyn osuusmaksun. Osuuskaupan jäsenet ovat keskenään samanarvoisia, sillä päätösvaltaa osuuskaupassa käytetään ääni/jäsen -periaatteella. Pirkanmaan Osuuskauppa on jäsenmäärältään toiseksi suurin alueosuuskauppa. Sillä oli vuonna 2011 noin 160 000 jäsentä. (S-kanava: omistusrakenne, S-kanava: yritysprofiili)

Ketjutoimintaperiaate

S-ryhmän liiketoimintamalli perustuu ketjutoimintaperiaatteelle, mikä tarkoittaa, että SOK toimii osuuskauppojen keskusliikkeenä ja tuottaa osuuskaupoille hankinta-, asiantuntija- ja tukipalveluita sekä vastaa S-ryhmän strategisesta ohjauksesta ja eri ketjujen kehittämisestä. Ketjuliiketoiminta mahdollistaa muun muassa laajojen valikoiminen hallinnan ja suuret hankintaerät sekä erityisammattitaidon tarjoamisen osuuskaupoille. S-

ryhmän valtakunnallisia ketjubrändejä ovat muun muassa Prisma, S-market, Sale ja ABC. Ketjuohjausorganisaatio vastaa oman toimialansa ketjutoiminnan koordinoinnista, kehittämisestä, ohjaamisesta ja valvonnasta. Alueosuuskaupat itsenäisinä yrityksinä voivat kuitenkin ketjuohjauksesta huolimatta hyödyntää paikallisen markkina- ja asiakastuntemuksensa. (S-kanava: yritysprofiili, S-kanava: ketjut ja palvelut)

Hallinto ja johto

Vaikka Pirkanmaan Osuuskauppa toimii osana S-ryhmää on se kuitenkin itsenäinen yritys, jolla on oma hallinto. Pirkanmaan Osuuskaupan keskeiset hallintoelimet ovat: asiakasomistajat, edustajisto, hallintoneuvosto, hallitus ja toimitusjohtaja. Asiakasomistajat voivat vaikuttaa osuuskaupan toimintaan äänestämällä edustajiston vaaleissa, toimimalla itse hallintoelimissä tai antamalla palautetta erilaisia palautekanavia pitkin. (S-kanava, Pirkanmaa: hallinto ja johto)

Vaaleilla valitulle edustajistolle kuuluu ylin päätäntävalta asioissa, jotka sille lain ja sääntöjen mukaan on määrätty. Edustajisto muun muassa myöntää vastuuvapauden toimitusjohtajalle ja hallintoneuvoston sekä hallituksen jäsenille. Varsinaisen toimielinroolinsa lisäksi edustajistolla on merkittävä asema laajan kontaktipinnan muodostajana asiakasomistajien ja osuuskaupan johdon välillä. Pirkanmaan Osuuskaupan edustajistoon kuuluu 60 jäsentä, jotka valitaan vaalilla osuuskaupan jäsenistä joka neljäs vuosi. (S-kanava,:hallinto ja johto, S-kanava, Pirkanmaa: hallinto ja johto)

Pirkanmaan Osuuskaupan hallintoneuvostoon kuuluu 24 jäsentä. Hallintoneuvoston tehtävänä on valvoa, että osuuskauppaa ja sen hallintoa hoidetaan lain ja sääntöjen sekä edustajiston ja hallintoneuvoston päätösten mukaisesti. Hallintoneuvosto myös vahvistaa osuuskaupan strategian ja valitsee hallituksen jäsenet. (S-kanava: hallinto ja johto, S-kanava, Pirkanmaa: hallinto ja johto)

Pirkanmaan Osuuskaupan hallitukseen kuuluu kuusi jäsentä, joista viisi valitaan vuosittain. Hallituksen puheenjohtajana toimii osuuskaupan toimitusjohtaja osuuskunnan sääntöjen mukaisesti. Hallituksen tehtävänä on ohjata liiketoimintaa siten, että sillä edistetään osuuskaupan etua ja menestystä. Lisäksi hallitus valvoo, että yrityksessä toimitaan lain, sääntöjen ja edustajiston sekä hallintoneuvoston antamien ohjeiden ja päätösten mukaisesti. Hallitus vastaa viime kädessä osuuskaupan liiketoiminnan menestyk-

sellisyydestä, joten se myös päättää osuuskaupan keskeiset tavoitteet, strategiat ja investoinnit. Toimitusjohtajan vastuulla on osuuskaupan johtaminen lain ja sääntöjen sekä hallintoelinten päätösten ja ohjeiden mukaisesti. (S-kanava: hallinto ja johto, S-kanava, Pirkanmaa: hallinto ja johto)

4.2 Empiirisen aineiston kerääminen ja analysointi

Tutkimuksen aineisto kerätään teemahaastatteluin, joiden pohjalta mallinnetaan kohdeyrityksen nykyinen riskienhallintajärjestelmä ja sen kehittämiskohteet. Haastattelujen avulla kartoitetaan lisäksi yrityksen toiveita riskienhallintaan liittyen. Teemahaastatteluilla pyritään saamaan merkityksellisiä vastauksia tutkimuksen ongelmanasettelun kannalta. Haastatteluissa käytettävät teemat perustuvatkin tutkimuksen viitekehykseen.

Teemahaastattelulla tarkoitetaan nimensä mukaisista haastattelumuotoa, jossa keskitytään tiettyihin teemoihin (Tuomi & Sarajärvi 2009, 75). Hirsjärvi & Hurme (2011, 47) kuvaavat teemahaastattelua lomakehaastattelun ja strukturoimattoman haastattelun välimuodoksi. Teemahaastattelulle on tyypillistä, että haastattelun aihepiirit eli teema-alueet ovat tiedossa, mutta kysymysten tarkka muoto ja järjestys puuttuvat (Hirsjärvi, Remes & Sajavaara 2004, 197). Hirsjärvi ja Hurme (2011, 48) esittävät teemahaastattelun eduksi sen, että yksityiskohtaisten kysymysten sijaan haastattelu etenee keskeisten teemojen varassa tuoden tutkittavien äänen paremmin kuuluviin. Teemahaastattelu huomioikin ihmisten erilaiset tulkinnat asioista.

Haastattelu voidaan toteuttaa yksilö-, pari- tai ryhmähaastatteluna (Hirsjärvi, Remes & Sajavaara 2004, 199). Tutkimuksessa käytetään sekä pari- että yksilöhaastattelua. Molemmissa haastattelutavoissa on omat etunsa. Yksilöhaastattelussa voidaan keskittyä yksin haastateltavaan ja saada esiin haastateltavan näkemys ilman, että ryhmässä toinen henkilö dominoisi toista. Haastattelussa, jossa on enemmän kuin yksi haastateltava, on haastateltavilta kuitenkin mahdollista saada enemmän ja tarkempaa tietoa. Haastateltaville saattaa tulla mieleen asioita, joita he eivät muuten huomaisi mainita. Lisäksi haastattelutilanne on usein luontevampi ja haastateltavat kokevat olonsa vapautuneemmaksi, kun useampia henkilöitä on paikalla. Parihaastattelu on lisäksi ajankäytöllisesti tehokas

haastattelumuoto. (Eskola & Suoranta 1998, 87–105; Hirsjärvi, Remes & Sajavaara 2004, 199).

Haastatteluissa keskeisessä roolissa ovat ne yrityksen henkilöt, joilla on eniten käytännön tietoa yrityksen riskienhallinnan järjestelmästä sekä ne, joilla on päätösvaltaa riskienhallinnan kehittämisessä. Täten haastateltaviksi valikoituivat kohdeyrityksen johtoryhmä henkilöstöjohtajaa lukuun ottamatta sekä hallituksen kaksi jäsentä. Kohdeyrityksen ketjuorganisaatioluonteesta johtuen tutkimukseen haastatellaan kuitenkin myös keskusliikkeen riskienhallinnan asiantuntijoita. Haastatteluiden lisäksi tutkija pohtii tutkimuksen olennaisimpia kysymyksiä yhdessä kohdeyrityksen toimitusjohtajan ja talousjohtajan kanssa.

Aineiston analysointi

Laadullisen aineiston analyysitapoja on useita. Tapaustutkimuksen yleisimmin käytettyjä menetelmiä ovat luokittelu, kategorisointi ja teemoittelu. Aineiston analyysitavan valintaan vaikuttaa tutkimuksen tavoite ja tarkoitus. (Eriksson & Koistinen 2005, 30) Tässä tutkimuksessa aineiston data teemoitellaan teoriaosuudessa esitetyn riskienhallintamallin osa-alueiden mukaisesti. Teoreettinen viitekehys toimii siis analyysia ohjaavana tekijänä.

Aineiston analyysi toteutetaan vaiheittain seuraavasti:

1. Haastatteluaineiston purkaminen analysoitavaan muotoon;
2. Aineistoon perehtyminen;
3. Aineiston järjestäminen, teemoittelu;
4. Tulosten tulkinta.

Haastatteluaineisto ensin litteroidaan sanatarkasti, jonka jälkeen aineistoon perehdytään nauhojen kuuntelulla ja aineiston läpilukemisella siten, että aineiston kokonaisuus avautuu tutkimusongelmaan nähden. Aineiston järjestäminen teemoittain mahdollistaa tutkimusongelmaa valaisevien teemojen nostamisen esiin aineistosta. Aineistoa analysoimalla löydetään kohdeyrityksen riskienhallinnan ongelmakohdat ja kehityskohteet, minkä jälkeen tutkimuksen tuloksissa esitetään riskienhallinnan tavoitetila ja kehitysehdotukset.

4.3 Tutkimuksen laadun arviointi

Tutkimuksen luotettavuuden arviointi on olennainen osa tutkimusta. Luotettavuutta arvioitaessa kiinnitetään erityisesti huomiota tutkimuksen toistettavuuteen. Taustalla on ajatus, että tutkimusten tulosten tulisi olla ei-sattumanvaraisia. Erityisesti laadullisten tutkimusten osalta tutkimuksen toistaminen ei kuitenkaan ole aina mahdollista. Lisäksi jos laadullinen tutkimus perustuu haastatteluin kerättyyn aineistoon, on tutkimuksen toistettavuus usein vielä hankalampaa. Haastatteluaineisto on aina konteksti- ja tilannesidonnainen, mikä tarkoittaa sitä, että tutkittavat saattavat puhua haastattelutilanteessa toisin kuin jossakin toisessa tilanteessa. Tämä pitääkin huomioida tutkimuksen toistettavuutta ja validiutta arvioitaessa. (Hirsjärvi, Remes & Sajavaara 2004, 196, 216–217) Tutkimuksen luotettavuutta onkin tässä pyritty parantamaan tarkalla selostuksella tutkimuksen vaiheiden toteuttamisesta ja aineistosta. Lisäksi tutkija on tarkastanut litteroimansa haastattelut kuuntelemalla samanaikaisesti nauhoituksia ja lukemalla litteroituja tekstejä.

Tutkimuksen luotettavuutta arvioitaessa tulee lisäksi kiinnittää huomiota tutkimuksen validiuteen. Validiteetilla tarkoitetaan tutkimusmenetelmän kykyä tutkia juuri sitä, mitä tutkimuksessa on tarkoituskin tutkia. (Hirsjärvi, Remes & Sajavaara 2004, 214) Tutkimuksen haastattelukysymykset ja -teemat on johdettu tutkimuksen teoreettisen viitekehyksen sekä kohdeyrityksen toimitusjohtajan ja talousjohtajan kanssa käytyjen keskusteluiden pohjalta ja näin niiden pätevyys tutkimusongelmaan nähden on hyvä. Validiteetilla viitataan myös tutkimustulosten tarkkuuteen. Laadullisen tutkimuksen osalta on tarkoituksenmukaisempaa puhua tutkimustulosten ja havaintoaineiston tulkinnan pätevyydestä. (Alasuutari 1995, 153) Havaintoaineiston tulkinnan pätevyys on pyritty varmistamaan tutkittavaa ilmiötä käsitteleviin tutkimuksiin tutustumalla sekä tutkijan ja kohdeyrityksen tekemillä arvioinneilla.

4.4 Riskienhallinnan nykytila ja sen kehityskohteet

Kohdeyrityksen riskienhallinnan arvioinnissa hyödynnetään sisäisen tarkastuksen arvioinnin kriteereitä. Niiltä osin, kun riskienhallinta ei vastaa arviointikriteereitä, pyritään löytämään teoriaosuudessa esitetyn toimivan riskienhallintajärjestelmän mallin avulla kohteet, joita kehittämällä yrityksen riskienhallinta vastaa paremmin sisäisen tarkastuksen vaatimuksia.

POK toimii ympäristössä, jossa muutoksia tapahtuu nopeallakin tempolla ja riskeihin varautuminen on välttämätöntä. Sen toimintaan vaikuttavat vahvasti kotitalouksien kulutuskäyttäytyminen, hintojen vaihtelut, kilpailijat, työttömyysaste sekä muu taloudellinen epävarmuus. Näiden aiheuttamien riskien ohella POK:n tulee yhä enemmän kiinnittää huomiota sen liiketoiminnan sisältöön liittyviin riskeihin. Lisäksi S-ryhmällä on suuri maineriski, mikä heijastuu myös POK:n toimintaan. S-ryhmän markkinajohtajuus päivittäistavarakaupassa aiheuttaa sen, että toimintaa seurataan tiiviisti organisaation ulkopuolella. Pienikin virhe tuo huonoa julkisuutta ja voi vaikuttaa hyvinkin paljon yksittäisten osuuskauppojen toimintaan. Toimintaympäristön nopeat muutokset ja maineriskin suuruus aiheuttavatkin paineita tarkastella riskejä kokonaisvaltaisemmin sekä hallita niitä tehokkaammin.

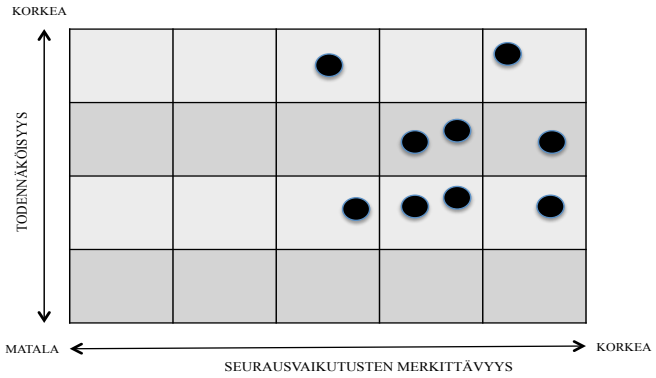
Osuuskuntatoiminta poikkeaa monessa niin sanotusta normaalista yritystoiminnasta. Esimerkiksi osakeyhtiömuotoisen yritystoiminnan päätavoite on mahdollisimman suuren voiton tuottaminen sen omistajille. Osuuskunnan päätavoitteena ei ole samassa mielessä voiton tuottaminen omistajille, vaan sen jäsenten tarvitsemien palvelujen mahdollisimman tehokas ja tarkoituksenmukainen aikaansaaminen. Jos voittoa, jota osuustoiminnassa kutsutaan ylijäämäksi, kuitenkin syntyy sen jälkeen, kun tarvittavat varaukset yrityksen kehittämiseksi on tehty, jaetaan se jäsenille siinä suhteessa, kun he ovat käyttäneet osuuskunnan palveluja. (Skurnik 2002, 6). POK:n jäsenten eli asiakasomistajien mahdollisimman hyvä palvelu edellyttääkin järkevää liikkeenjohtamista, jonka osa riskienhallinta puolestaan on. Riskienhallinnan merkitys osana arvon tuottamista ja menestymistä nähdään hyvin oleellisena erityisesti pitkällä tähtäimellä.

Vaikka voiton tavoittelu ei olekaan osuustoiminnan kulmakivi, eikä liian isoja riskejä olla edes välttämättä halukkaita ottamaan, voi liiallinen turvallisuushakuisuuskin koitua yrityksen tappioksi mikäli potentiaalisia mahdollisuuksia jää hyödyntämättä. Riskinotosta halutaankin tehdä POK:ssa mahdollisimman järkevää ja harkittua, jolloin myös suurempien riskien ottaminen ja potentiaalisiin mahdollisuuksiin tarttuminen mahdollistuu. Kokonaisvaltainen riskienhallinta on tapa, jolla riskejä voidaan tarkastella harkitummin ja kokonaisvaltaisemmin. SOK:ssa on jo siirrytty kokonaisvaltaiseen riskienhallintaan ja myös POK:ssa yhä enemmän kiinnitetään vahinkoriskien ohella huomiota strategisiin ja taloudellisiin riskeihin.

Riskienhallinnan kehittäminen nähdään siis ennen kaikkea tulevaisuuden menestymisen ja toiminnan jatkuvuuden edellytyksenä. Tavoiteltaessa tehokkaampaa ja toimivampaa riskienhallintaa pitää yrityksellä olla käsitys toimintaansa liittyvien riskien kokonaisuudesta sekä niiden kartoittamiseen soveltuvista käytännöistä. Yrityksessä tulee kuitenkin ennen kaikkea olla mietittynä, miten riskienhallinnasta saadaan luonnollinen osa kokonaisuutta siten, ettei se jää vain erilliseksi, lisäkustannuksia tuottavaksi palikaksi.

4.4.1 Riskienhallintaprosessi

Koko yrityksen tasolla riskitarkasteluiden ytimen muodostaa kuvion 4 mukainen kartta, jossa riskejä arvioidaan niiden seurausvaikutusten ja todennäköisyyksien pohjalta. Riskin seurausvaikutus ja todennäköisyys kerrotaan keskenään ja näiden tulona syntynyt luku kuvaa riskin suuruutta. Riskitarkastelut perustuvat riskien kokonaisuuden tarkasteluun ja näin myös riskien syy-seuraussuhteet huomioidaan. Kartta muodostuu lähinnä toimitusjohtajan ja talousjohtajan keskusteluiden ja pohdintojen tuloksena. Muu johtoryhmä ja hallitus osallistuvat työhön kommentoimalla kaaviota sekä ehdottamalla siihen mahdollisesti muutoksia. Lopulta hallitus hyväksyy riskikartan strategian yhteydessä ja hallintoneuvos vahvistaa sen. Seuraavana vuonna riskikarttaa päivitetään tarvittaessa. Yrityksen riskitarkasteluiden lähtökohta on liiketoiminnassa. Riskitarkasteluissa pyritäänkin siis tunnistamaan riskejä, jotka vaikuttaisivat negatiivisesti liiketoimintaan. Ongelmaksi on kuitenkin koettu ettei yrityksen riskitarkastelut perustu riittävästi toimialojen riskitarkasteluille



Kuvio 4 Riskikartta

Vuotuisten riskitarkasteluiden lisäksi yrityksessä tehdään vuotuisia toimialakohtaisia analyysejä, jotka perustuvat pääosin SWOT- ja ympäristöanalyyseihin. Nämä analyysimuodot mahdollistavat riskien tarkastelun tai ainakin riskinäkökulman huomioimisen, vaikka ne eivät varsinaisesti riskianalyysejä olekaan. Liiketoimintajohto kuitenkin kokee analyysit riittämättömiksi riskienhallinnan kannalta ja pitääkin strategisten riskien tunnistamista ja analysointia haasteellisena. Lisäksi riskienhallinnan organisoimattomuus toimialatasolla on johtanut siihen, että riskejä katsotaan läpi sormien ja riskit otetaan ikään kuin annettuina. Vaikka liiketoimintatasolla siis tunnistettaisiinkin riskejä, jätetään ne mahdollisesti huomioimatta ilman tarkempia riskianalyysejä, koska niiden ei ajatella vaikuttavan yrityksen toimintaan. Tämä väistämättä aiheuttaa sen, että jossain vaiheessa mahdollisuuksia jää hyödyntämättä tai riski, jolla on negatiivisia vaikutuksia yrityksen toimintaan, realisoituu.

Sisäinen tarkastus tekee operatiivisten riskien hallintaa POK:n yksiköissä. Operatiivisten riskien hallinta on selvästi systemaattisempaa kuin strategisten riskien hallinta. Operatiivisen tason riskien hallintaan on olemassa proseduureja, miten riskienhallintaa tulee tehdä. Lisäksi riskienhallinta pyrkii tältä osin olemaan myös ennakoivaa, vaikka toiminta perustuukin vielä nykyään aika paljon sille, että tilanteisiin tartutaan sitä mukaa kuin niitä ilmenee.

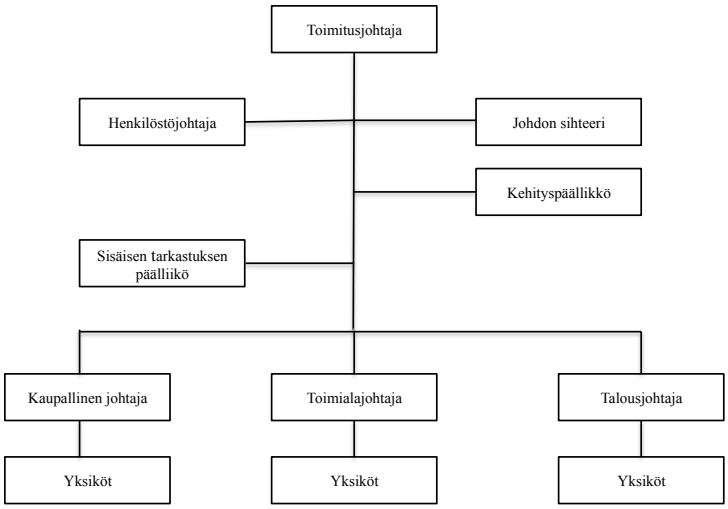
Verrattaessa POK:n riskienhallintaprosessia yleisten viitekehysten prosessikuvauksiin huomataan, että yrityksen riskienhallinta ei täytä kaikkia prosessin vaiheita. Koko yrityksen tasolla riskienhallinta on kuitenkin huomattavasti pidemmälle vietyä kuin toimialatasolla. Yrityksen tasolla riskejä pyritään tunnistamaan, analysoimaan ja toimintaa

mukautetaan suunnitteluvaiheessa riskien mukaan. Yrityksessä ei kuitenkaan seurata riskejä tai riskienhallinnan toteuttamista, mistä aiheutuukin ettei riskikartalla ole juuri käytännön hyötyä suunnitteluvaiheen jälkeen ja riskienhallinta onkin luonteeltaan lähinnä tilanteeseen reagoivaa, ei ennakoivaa tai jatkuvaa. Toimialatasolla riskienhallinta on myöskin kertaluonteista analyysien osalta. Liiketoimintajohdon on kuitenkin pakko analyysien lisäksi arvioida toimintansa riskejä ainakin jollain tasolla myös arkipäiväin liiketoiminnassa, mutta tätä ei tiedosteta varsinaisesti riskienhallinnaksi. Liiketoimintajohto siis tiedostamattaan arvioi riskejä ja peilaa toimintaansa riskeihin, mutta se ei ole systemaattista, joten tilanteiden analysoiminen jää usein puutteelliseksi, eikä riskeihin mietitä riittävästi ratkaisuja. Yrityksen riskienhallintaprosessit eivät täytäkään sisäisen tarkastuksen kriteereitä, joiden mukaan riskienhallinnan tulisi olla jatkuvaa, systemaattista ja jäsenneltyä.

Riskienhallintaprosessin näkökulmasta riskienhallinnan tärkeimpiä kehityskohteita ovatkin muodollisen riskienhallintaprosessin muotoilu, ohjeistuksen laatiminen, riskianalyysimallin rakentaminen sekä seurantajärjestelmien kehittäminen. Lisäksi prosessin yhtenäistäminen vaatii kommunikointia ja viestintää.

4.4.2 Organisaatiokulttuuri

POK:n organisaatiorakenne on hierarkkinen ja johtamisjärjestelmä on tarkkaan määritelty. Organisaatio on muodoltaan linjaorganisaatio (kuvio 5). Linjaorganisaation tunnusmerkki on, että toimivalta on keskitetty ylimmälle johdolle. Organisaatiossa ohjeita saadaan aina ylempänä toimivalta esimieheltä ja tieto kulkee organisaatiossa vain yhteen suuntaan: ylhäältä alaspäin. (Viitala 2004, 116)



Kuvio 5 Pirkanmaan Osuuskaupan organisaatiorakenne

Haastatteluiden perusteella voidaan kuitenkin todeta, että hierarkkisesta organisaatiorakenteesta huolimatta yrityksessä toimitaan hyvinkin lähellä toisia, eikä hierarkkisuus näy yrityksen arjessa. Haastateltavat luonnehtivat organisaatiokulttuuria avoimeksi, moderniksi ja välittömäksi. Lisäksi esille nousi tiimityöskentelyn merkitys yrityksen toiminnassa. Organisaatiokulttuurin edelleen kehittämiseksi on POK:n uusiin toimitiloihin rakennettu tiimihuoneita. Tiimihuoneiden ajatuksena on kommunikoinnin ja oppimisen lisääminen niin johtoryhmässä kuin muissakin yrityksen tiimeissä.

Pääosin haastateltavat näkivät yrityksen organisaatiokulttuurin tukevan tehokasta riskienhallintaa, sillä ilman avointa kommunikointia tärkeitäkin asioita saattaisi jäädä huomioimatta. Avoin ja vapaa kulttuuri nähtiin kuitenkin osittain myös huonoksi, koska sen koetaan ajavan organisaatiota mukavuudenhaluisuuteen ja vastuuttomuuteen. Ilman selkeää vastuiden jakamista toiminnan onkin vaikeaa olla tehokasta. Avoin kulttuuri on hyvän riskienhallinnan lähtökohta, mutta vaatii toimiakseen myös politiikkoja ja ohjeita, joiden mukaan toimitaan.

Riskikulttuurista ei kuitenkaan voida yrityksessä puhua. Riskienhallinta on enemmänkin kertaluonteinen projekti kuin kulttuuri. Lisäksi riskit nähdään yrityksessä edelleen enemmän uhkina kuin mahdollisuuksina. Sellaisen kulttuurin luominen, jossa riskienhallinta nähdään mahdollisuutena tehdä rohkeampia päätöksiä sekä kasvattaa liiketoiminnan arvoa, vaatii paitsi systemaattisen riskienhallintaprosessin olemassaoloa myös

onnistumisia riskienhallinnan saralla. Riskityön tuleekin olla tavoitteellista ja sitä tulee seurata, jotta riskienhallinnan hyödyt voidaan konkreettisesti osoittaa ja näin sitouttaa organisaatiota yhä parempaan riskienhallintaan.

4.4.3 Riskienhallinnan ohjeistus

POK:lla ei ole omaa kirjallista riskienhallintapolitiikkaa, jolle riskienhallinnan työ rakentuisi. Riskienhallinta perustuukin yrityksessä enemmän toteutuneeseen käytäntöön sekä toimitusjohtajan ja talousjohtajan vuosittain tarpeelliseksi katsomille asioille, jotka sitten ohjaavat yrityksen strategiaprosesseissa huomioitavia asioita. Ohjeistus riskienhallinnasta on myös muilta osin hyvin puutteellinen yrityksessä. POK:lla on käytössä S-ryhmän kokonaisvaltaisen riskienhallinnan kaavio, jonka avulla voidaan riskejä jäsennellä ja analysoida, mutta kaavion käyttö rajoittuu kerran vuodessa tehtävän riskikartan rakentamiseen. Lisäksi suurien vahinkoriskien varalle yrityksessä on S-ryhmän laajuiset toimintaohjeet.

SOK on tehnyt kaikille osuuskaupoille yhteisen riskienhallintapolitiikan, jossa on otettu kantaa niihin keskeisiin asioihin, joita osuuskauppojen tulisi riskienhallintatyössään huomioida. Politiikassa määritellään muun muassa riskienhallintaprosessi ja riskienhallinnan vastuut. SOK:n tekemä riskienhallintapolitiikka on sekä suositus siitä, miten riskienhallinnan työtä tulisi tehdä, mutta sen on tarkoitus myös tukea osuuskauppojen oman riskienhallintapolitiikan muotoilua. Tämän käytännön hyöty on kuitenkin jäänyt POK:ssa vähäiseksi, eikä tällaisen dokumentin olemassaolosta olla yleisesti tietoisia.

Ohjeistuksen puute on johtanut siihen, että riskejä ei tarkastella riittävästi ja niitä katsotaan osittain jopa läpi sormien. Riskienhallinnan tavoitteista ja vastuista ei ole selkeää ymmärrystä eikä riskienhallinta ole yhtenäistä. Riskeihin suhtautuminen onkin tällä hetkellä pitkälti tilanne- ja henkilökohtaista. Henkilökohtaisella tarkoitetaan tässä sitä, että ihmisestä riippuen riskejä kartetaan tai vaihtoehtoisesti otetaan huolimattomasti liiankin paljon riskiä. Riskienhallintapolitiikalla riskienhallinnan koko kenttää voidaan huomattavasti selkiyttää. Siinä linjataan muun muassa riskienhallinnan vastuut ja tavoitteet. Riskistrategialla puolestaan voidaan yhtenäistää yrityksen sisällä riskikäsitystä ja riskei-

hin suhtautumista. Lisäksi riskienhallinnan käytännön työ vaatii tuekseen analyysimallin, jolla riskejä voidaan tarkastella systemaattisemmin.

Riskistrategian lisäksi riskeihin suhtautumista voidaan ohjata riskinkantokyvyn määrittelyllä. POK:n talousjohtaja tekeekin arvioita yrityksen riskinkantokyvystä testaamalla tuloslaskelman ja taseen kykyä sietää erilaisia skenaarioita. Lopulta kuitenkin näiden testausten hyödyntäminen käytännön riskienhallintatyössä yrityksen muilla tasoilla jää suhteellisen pieneksi, eikä ne varsinaisesti ohjaa riskienhallintatyötä. Arvoa näillä laskelmilla kuitenkin on muun muassa investointipäätösten yhteydessä. Investointeja ja niiden rahoittamista pohdittaessa huomioidaan muun muassa käyttökatteen kriittinen piste eli tarkastellaan, kuinka paljon käyttökate voi pudota ilman, että joudutaan priorisoimaan tai lykkäämään investointeja. Raportoimalla näistä talousjohtajan tekemistä testauksista, voitaisiin riskienhallintakykyä myös käyttää riskinottoa ohjaamaan.

4.4.4 Riskienhallinnan vastuut ja sisäinen viestintä

Strateginen riskienhallinta on tällä hetkellä lähinnä talousjohtajan vastuulla. Strategisen ja taktisen tason riskienhallinnan vastuita ei ole varsinaisesti yrityksessä jaettu tai liitetty työnkuvauksiin. Esimerkiksi liiketoimintajohdon osalta on oletus, että riskienhallinta on yksi osa johdon työnkuvaa. Riskienhallinnan yhdeksi suurimmista ongelmista koettiinkin se, ettei riskienhallinnan koordinointi ole kenenkään toimenkuvassa pääasiana ja näin se onkin jäänyt vain strategian yhdeksi osaksi, jota ei kunnolla koordinoida yrityksessä. POK:ssa on tehty toimenkuvien päivitykset johdon, keskijohdon ja esimiesten rooleista ja näin pyritty selkiyttämään työnjakoa. Riskienhallinnan vastuiden määrittely kaipaisikin samankaltaista selkeää erittelyä. Lähempänä operatiivista toiminnan tasoa vastuunjako on kuitenkin huomattavasti selkeämpää. Seuraavassa on eritelty johdon, hallituksen ja sisäisen tarkastuksen riskienhallinnan työtä, joka tapahtuu lähinnä strategiasuunnittelun yhteydessä.

Johto

Riskienhallinnasta on viime kädessä vastuussa yrityksen toimitusjohtaja, vaikka riskienhallinnan vastuu onkin oletuksen mukaan jaettu eri johtamistasoille. Talousjohtaja vastaa strategiaprosessista, jonka osana riskitarkastelut tehdään. Toimitusjohtaja puoles-

taan antaa toimeksiannon strategian pohjana olevien analyysien tekemisestä toimialajohtajille. Toimialajohtajat yhdessä lähialaistensa kanssa rakentavat SWOT- ja ympäristöanalyysit, jonka jälkeen ne käsitellään johtoryhmässä. Ennen johtoryhmän istuntoa toimitusjohtaja käy vielä kahden kesken toimialajohtajien kanssa analyysit läpi, ja niitä hiotaan tarvittaessa. Johtoryhmän istunnon jälkeen, ennen kuin analyysit esitellään hallitukselle, tarkastellaan vielä sen vuoden strategian painotukset.

Näiden toimialakohtaisten analyysien lisäksi johtoryhmässä tehdään koko yrityksen näkökulmasta riskiarviointi eli arvioidaan, mitä riskejä yrityksellä on, ja mitkä ovat riskien vaikutukset ja todennäköisyydet. Liiketoimintajohdolla on kuitenkin suhteellisen löyhä suhde riskienhallintaan, koska sille ei ole varsinaisesti annettu vastuuta tästä, ja talousjohtaja yleensä yhdessä toimitusjohtajan kanssa tuokin asiat esille ja niistä sitten keskustellaan yhdessä.

Hallitus

Hallituksen tehtävä on valvoa ja kyseenalaistaa riskienhallinnan toimintaa. Hallitus on viime kädessä vastuussa liiketoiminnassa, joten sen tuleekin olla kriittinen riskienhallinnan suhteen. Riskienhallinnan arviointiin ei hallituksella ole mitään selkeää kaavaa tai mittaristoa, vaan se perustuu pikemminkin keskusteluihin ja kokemustaustoihin. Hallitus käsittelee kerran vuodessa sisäisen tarkastuksen riskiraportin sekä tulevan vuoden suunnitelman. Hallitus myös hyväksyy koko yrityksen sekä sen toimialojen strategiat ja antaa niihin tarvittaessa muutosehdotuksia. Näiden lisäksi ajankohtaiset muutokset ja riskit tulevat hallituksen käsiteltäväksi. Muun muassa isot investoinnit tulevat sen käsiteltäviksi useassa vaiheessa ja niistä käydään keskustelua ennen kuin valmiiseen investointisuunnitelmaan asti päästään. Tämä keskustelu nähdään osana riskienhallintaa.

Hallitus on kuitenkin jokseenkin passiivinen yrityksen riskienhallinnan valvonnassa. Hallitus lähinnä olettaa, että sen tarvitsema riski-informaatio annetaan sille automaattisesti johdon harkinnan mukaan. Osittain tämä oletus perustuu hallituksen kokoonpanoon, jossa hallituksen puheenjohtajana on yrityksen toimitusjohtaja. Hallituksella ei kuitenkaan ole täysin selvää kuvaa siitä, miten johtoryhmässä riskejä käsitellään. Hallituksen tulisikin ottaa näiltä osin aktiivisempi rooli riskienhallinnan valvojana. Hallitus myös kokee, että riskeistä olisi hyvä raportoida heille useammin, esimerkiksi neljännes-

vuosittain tai kahdesti vuodessa. Lisäksi se kaipaisi enemmän tietoa siitä, miten riskit ovat kehittyneet, miten riskit ovat vaikuttaneet yrityksen toimintaan sekä, miten riskeihin on vastattu.

Sisäinen tarkastus

POK:n sisäisen tarkastuksen vastuulla on yrityksen operatiivisten riskien hallinta. Käytännössä sisäinen tarkastus tekee siis tarkastuksia POK:n yksiköissä. Operatiivisten riskien osalta riskienhallintatyö on systemaattista ja sen tasoon ollaan organisaatiossa yleisesti tyytyväisiä. Ero strategisen tason riskienhallintaan on se, että operatiivisten riskien hallinta on usein selkeämpää, mutta lisäksi siihen on varattu yrityksessä selkeästi omat resurssit. Yrityksen suurimmat riskit eivät kuitenkaan ole operatiivisella tasolla, joten riskienhallinnan strategisen tason työhön on tulevaisuudessa panostettava enemmän.

Sisäinen viestintä

Vuotuinen riskienhallinnan työ kiteytyy johtoryhmän muotoilemaan riskikarttaan. Riskikartta käsitellään alajohtoryhmässä, johtoryhmässä ja hallituksessa sekä hallintoneuvostossa, joka vahvistaa sen. Riskikartan ohella yrityksessä raportoidaan hallitukselle yksiköiden operatiivisista riskeistä. Näiden vuotuisten raportointien lisäksi riskeistä keskustellaan aina jollain tasolla myös hankkeiden yhteydessä. Keskustelu riskeistä ajoittuu erityisesti hankkeen suunnitteluvaiheeseen ja toisinaan tämä tapahtuu vain suullisesti ilman dokumentaatiota. Yrityksen taloudellisista asioista raportoidaan hallitukselle kuukausittain. Sekä hallitus että johto ovat yhtä mieltä siitä, että myös riskeistä ja riskienhallinnasta tulisi raportoida hallitukselle useammin kuin kerran vuodessa. Kuukausittain olisi kuitenkin niin johdon kuin hallituksen mielestä liian usein. Raportointiväli voisikin olla joko puolen vuoden tai kvartaalin välein.

Riskeistä puhutaan myös toimialatasolla, mutta niistä ei tehdä erillistä raporttia. Liiketoimintajohto analysoi riskejä omissa tiimeissään ja näin riskitietoisuuden pitäisi siirtyä organisaatiossa alaspäin. Riskitietoisuuden lisäämiseksi ja riskienhallintatyön selkiyttämiseksi myös toimialatasolla kaivattaisiin kuitenkin raportointia. Tällä hetkellä riskit ovatkin vain irrallinen osa-alue, joka käsitellään muiden asioiden yhteydessä, mutta varsinaisesti riskeistä ja riskienhallinnasta pelkästään ei koskaan puhuta.

Kaikki haastateltavat olivat tietoisia siitä riskienhallinnan osasta, joka raportoidaan eli johtoryhmän muotoilemasta riskikartasta ja sisäisen tarkastuksen operatiivisten riskien selvityksestä. Muilta osin riskienhallinnan työstä osattiin sanoa vain omien tekemisten osalta. Toisin sanoen vaikka yrityksessä tehtäisiinkin asioita riskienhallinnan eteen, ongelma on ettei niistä viestitä yrityksessä muille. Keskustelu riskeistä koetaankin yrityksessä todella tärkeäksi, jotta uudet riskit voidaan tunnistaa ja voidaan varmistua siitä, että riskit nähdään samalla tavalla yrityksessä. POK:n riskienhallintatyön selkiyttäminen ja riskiymmärryksen lisääminen edellyttää keskustelun lisäksi myös systemaattisempaa raportointia. Viestintä on myös oleellinen osa sitouttamista. Raportointikäytännöistä tulisikin linjata yrityksen riskienhallintapolitiikassa.

4.4.5 Päätöksenteko

Selkeimmin riskit huomioidaan yrityksen toiminnassa päätöksenteon yhteydessä. Riskienhallinta ei siis perustu vain päätöksenteon seurausten hallintaan, vaan riskejä tarkastellaan jo suunnitteluvaiheessa. Riskien huomioiminen päätöksenteon yhteydessä tekeekin päätöksistä huomattavasti harkitumpia. Riskien tarkastelu päätöksiä tehtäessä perustuu kuitenkin päätöksentekijän omiin kykyihin ja kokemuspohjaan, koska yrityksessä ei ole muodollista riskianalyysia tai muutakaan ohjeistusta, joka ohjaisi päätöksentekoa. Riskejä ajatellaan yleensä kustannusten muodossa eli päätöksestä aiheutuvien kustannusten pitää pitää sisällään riskien mahdolliset kustannukset siltä varalta, että riskit realisoituisivatkin. Jos kustannukset sitten osoittautuvat liian suuriksi, projektista luovutaan, eikä päätöksentekoprosessia tällaisenaan viedä loppuun asti. Yleisesti hyväksyttävien kustannusten määrittäminen ei kuitenkaan perustu yrityksen riskinkantokykyyn. Suurempien päätösten osalta näin saattaa toki olla, koska talousjohtaja voi simuloida laskelmillaan yrityksen taseen ja tuloslaskelman kestävyyttä.

Vaikka riskit ovatkin mukana päätöksiä tehtäessä ja niitä suunniteltaessa, unohtuvat ne usein projektin edetessä. Tämä johtuukin osittain siitä ettei päätöksentekoon liittyvää riskitarkastelua useinkaan dokumentoida, ja toisinaan riskit mainitaankin vain suullisesti hallitukselle esittelemisen yhteydessä. Varsinaisesti riskien seurantaa ei siis tehdä lukuun ottamatta vuotuisia riskitarkasteluja. Riskienhallinnan prosessimallia tulisikin noudattaa myös päätöksenteon yhteydessä. Päätöksen riskit ensin tunnistetaan ja ne ana-

lysoidaan, mutta lisäksi niiden hallitsemiseksi tulisi tehdä aktiivisesti erilaisia toimenpiteitä ja toimenpiteiden vaikuttavuutta pitäisi seurata. Ja kaikki prosessin vaiheet tulisi dokumentoida. Lisäksi päätöksentekotilanteet vaativat tuekseen riskistrategian, joka ohjaa päätöksentekoa riskeihin suhtautumisen osalta. Riskinottokyvyn määrittelyllä voidaan myös ohjata riskipäätösten tekemistä. Riskianalyysimallin käyttämisellä puolestaan riskitarkasteluista ja -päätöksistä saadaan tehtyä systemaattisempia.

4.4.6 Johtamisjärjestelmä

Strategiasuunnittelu

POK:n strategia muotoillaan aina viideksi vuodeksi kerrallaan. Strategiat muotoillaan aina sekä koko yritykselle että toimialakohtaisesti. Koko yrityksen strategia muodostuu lähinnä toimialojen strategioiden summana, vaikkakin yritystason valinnat vaikuttavat myös yrityksen strategiaan. S-ryhmä ohjaa toimialakohtaisia strategioita ja määrittelee niille valtakunnallisen linjan. Koko yrityksen strategiassa tulee siis huomioida paitsi S-ryhmän linja myös toimialojen omat linjaukset. Ryhmärakenteesta johtuen POK:n strategia on siis pitkälti johdettu S-ryhmän strategiasta. Tästä seuraakin, että tärkeimmät strategiset valinnat tulee annettuina, jolloin myös riskien pohtiminen on enemmän sitä, mitä riskejä POK:n kannalta S-ryhmän määrittelemään strategiaan liittyy. POK:n tuleekin siis vain hienosäätää strategiansa markkinoihin sopivaksi ja huomioida siinä sen omat alueelliset riskit. SOK on strategiavalinnoissaan huomioinut riskit, ja strategiat ovat lähtökohtaisesti sellaisia, että ne eivät sisällä riskejä, jotka voisivat vaarantaa osuuskauppojen tavoitteiden saavuttamisen merkittävästi. Näin ollen POK:n vastuulla ei olekaan sen pohtiminen, ovatko strategiat järkeviä riskien kannalta. Kuitenkin yrityksen pitää pohtia sitä, miten strategioiden riskit voivat vaikuttaa yrityksen toimintaan ja sen resursseihin.

Strategian oheen piirretään lisäksi strategiaennuste siitä, mihin suuntaan toiminta on menossa ja, kuinka strategia toteutuu. Ennusteessa on huomioitu myös riskit. Joka vuosi tehdään strategian tarkastus, jossa tarkastellaan sitä, ollaanko toimittu, kuten on suunniteltu. Strategisen pohdinnan osana myös edellisenä vuonna linjattuja riskejä tarkistetaan sekä seurataan niiden toteutumista. Koska toimintaympäristö muuttuu jatkuvasti, pohdi-

taan tässä yhteydessä myös sitä, pitäisikö strategiaa mahdollisesti muokata muuttuneisiin olosuhteisiin, jolloin myös riskit voivat muuttua.

Tavoitteiden asettaminen ja seuranta

POK:n toiminta perustuu pitkälti tulosjohtamiseen. Tulosjohtamisessa peruskriteerinä on tulosten suhde asetettuihin tulostavoitteisiin, ja tuloksen tekeminen alistetaan arviointiin, joka suoritetaan tulosmittareilla. Riskienhallintaa ei ole erikseen huomioitu yrityksen tulostavoitteissa. Tulosjohtamisen osana käytetään tasapainotettua mittaristoa, jonka näkökulmat ovat asiakkaat, talous, prosessit ja henkilöstö. Tasapainotettu mittaristo on mukana vuosisuunnitelmissa ja tavoitteiden asettamisessa sekä jonkun verran kuukausittaisessa raportoinnissa. Tasapainotettu mittaristo on tullut yritykseen vaiheittain viimeisen vuosikymmenen aikana. Siihen ei ole olemassa vielä tietojärjestelmää, joten sen käyttö on toistaiseksi koettu työlääksi ja hankalaksi. S-ryhmällä on kuitenkin kehitteillä uusi prosessimalli, jonka osana on myös tasapainotettu mittaristo, ja sen tulisikin tulevaisuudessa helpottaa mittariston käyttöä.

Tasapainotettua mittaristoa käytetään kaikilla organisaatiotasoilla. Mittaristo on ketjuohjattu eli esimerkiksi kaikki ABC:t toimivat samalla mittaristopohjalla. Mittaristot ovat siis toimipaikka-, ketju-, ja yritystasoisia. Toimipaikkatasolla mittaristoa seurataan liiketoiminnassa ja se on osittain sidottu toimipaikkojen päälliköiden palkkioperusteisiin. Ketjutasolla tarkastellaan esimerkiksi S-market -ketjun ja Prisma-ketjun tuloskortteja, joissa on aina kolmen vuoden tavoitearvot eri mittareille. Yritystason mittarit ovat muiden tasojen mittaristoihin verrattuna hyvin yleisellä tasolla. Yritystasolla tarkastellaan muun muassa konsernitason tulosprosentteja ja omavaraisuusasteita. Tavoitteenasettelu lähtee kuitenkin POK:ssa kahdesta suunnasta liikkeelle: alhaalta ylöspäin ja ylhäältä alaspäin, mikä käytännössä tarkoittaa ettei esimerkiksi toimialatavoitteita pyritäkään pakottamaan alaspäin, vaan yksiköiden tavoitteet asetetaan toimialatavoitteista erillään ja sitten lopuksi katsotaan, mihin yksiköiden toiminnalla on päästy suhteessa yksiköiden tavoitteisiin ja suhteessa toimialojen tavoitteisiin.

Riskienhallinnan liittäminen tasapainotettuun mittaristoon nähdään mahdollisuutena integroida riskienhallinnan tavoitteet yrityksen muihin tavoitteisiin. Haastateltavista kaikki eivät kuitenkaan kokeneet tätä hyvänä ajatuksena, koska esimerkiksi tulosyksi-

köiden tuloskorteissa riskit ovat jo valmiiksi tavoitteiden sisään mietittyinä siinä vaiheessa, kun tavoitteet laitetaan tuloskorttiin. Kuitenkin jotta riskienhallinta voisi olla paremmin mukana yrityksen vuosijohtamisessa, tulee sille olla selkeät tavoitteet, joiden toteutumista seurataan. Ja jottei riskienhallinnan työstä tulisi vain tarkistuslistatyyppinen, kertaluonteinen projekti, pitää riskienhallinnan tavoitteet liittää osaksi yrityksen muuta tavoitteenasettelua ja seurantaa.

4.4.7 Riskienhallinnan seuranta ja arviointi

Riskienhallinnan tavoitteita ei ole selkeästi määritelty yrityksessä, minkä luonnollinen seuraus on ettei myöskään riskienhallintaa seurata tai arvioida sen enempää. Asia voidaan nähdä myös toisinpäin: Riskienhallintaa ei arvioida yrityksessä, joten se ei myöskään voi olla tavoitteellista eikä jatkuvan parantamisen ajatuksen mukaista. Riskienhallinnan seurantaan ja arviointiin pitääkin olla järjestelmät, joilla varmistetaan jatkuvan parantamisen periaatteen mukainen toiminta. Riskienhallinnan tavoitteiden liittämisellä osaksi tasapainotettua mittaristoa voidaan tavoitteiden toteutumista seurata ja arvioida ilman uusien järjestelmien kehittämistä.

Edellä esitetyt riskienhallinnan ongelmat ja kehityskohteet on koottu yhteenvetona taulukkoon 1. Taulukko noudattelee samaa jaottelua kuin tutkimuksen teoreettinen viitekehys.

	Ongelma	**Kehityskohde**
Riskienhallintaprosessi	Systemaattisuuden puute Kertaluonteisuus Prosessin vajavaisuus Seurannan puute Riskienhallinnan organisoimattomuus	Ohjeistus, Viestintä & kommunikointi Muodollinen riskienhallintaprosessi Riskianalyysimalli Seurantajärjestelmä
Organisaatiokulttuuri	Vastuuttomuus Riskikulttuurin puute	Vastuiden selkiyttäminen Muodollinen riskienhallintaprosessi Tavoitteet Seurantajärjestelmä
Riskienhallinnan ohjeistus	Ohjeistus puuttuu Systemaattisuuden puute Riskienhallinnan tavoitteiden ja vastuiden epäselvyys Riskinkantokyky ei ohjaa riskinottoa	Riskienhallintapolitiikka Riskistrategia Riskianalyysimalli Viestintä
Riskienhallinnan vastuut ja sisäinen viestintä	Riskienhallintaa ei koordinoida Vastuut epäselvät Raportoinnin vähäisyys	Riskienhallintapolitiikka Viestintä
Päätöksenteko	Systemaattisuuden puute Riskinkantokyky ei ohjaa päätöksentekoa Dokumentaation puute Riskien tarkastelu suunnitteluvaiheen jälkeen puuttuu	Riskianalyysimalli Muodollinen riskienhallintaprosessi Riskinkantokyvyn määrittely Riskistrategia Dokumentointi
Johtamisjärjestelmä	Riskienhallinnan tavoitteet erillään muista toiminnan tavoitteista	Tasapainotettu mittaristo
Seuranta ja arviointi	Seurannan ja arvioinnin puute	Tasapainotettu mittaristo

Taulukko 1 Riskienhallinnan kehityskohteet

5 TUTKIMUKSEN KESKEISET TULOKSET

5.1 Riskienhallinnan tavoitetila

POK:ssa riskienhallinta perustuu kerran vuodessa tehtävään riskien arviointiprojektiin sekä riskitarkasteluihin päätöksenteon ja suunnittelun yhteydessä. Riskienhallinta ei kuitenkaan ole jatkuvaa, koska riskien tarkastelu rajoittuu pääasiassa vain suunnitteluvaiheeseen. Riskienhallinta tulisikin integroida selvemmin yrityksen toimintoihin, jotta se todella olisi osa yrityksen normaalia toimintaa. Tämä vaatii huomattavasti nykyistä tarkemmat proseduurit ja ohjeistukset tuekseen. Lisäksi sekä muutoksen toteuttaminen että riskienhallinnan tekeminen tulevaisuudessa rakentuu vahvasti viestinnälle. Raportoinnilla varmistetaan riskitietoisuuden leviäminen yrityksessä ja näin tuetaan aidon riskikulttuurin syntymistä. Viimeisenä palikkana on riskienhallinnan seuranta ja arviointi. Niiden avulla on mahdollista varmistua, että yritys todella toteuttaa riskienhallintaa tehokkaalla ja toimivalla tavalla, ja toisaalta vain näin voidaan mahdollistaa toiminnan jatkuva parantaminen.

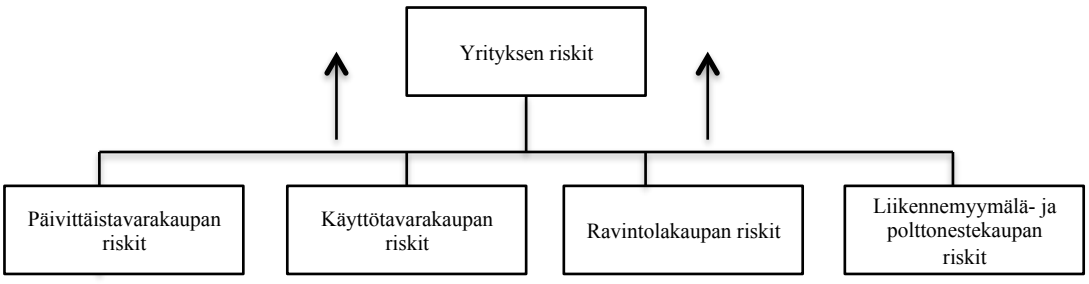
Nykytilan analysoinnin ja haastatteluissa esille tulleiden kehitysajatusten pohjalta on seuraavassa konstruoitu riskienhallinnan malli, jolla riskienhallinnasta saadaan muodostettua tehokkaampi ja toimivampi järjestelmä kohdeyrityksessä. Yrityksen riskienhallinnan kehittämiskohteet voidaan karkeasti jakaa neljään osa-alueeseen: riskienhallintaprosessi, ohjeistus, tasapainotettu mittaristo ja viestintä.

Riskienhallintaprosessi

Yrityksellä pitää olla ennen kaikkea olemassa muodollinen riskienhallintaprosessi, johon koko riskienhallinta kiteytyy. Riskienhallintaprosessin avulla yrityksessä hahmottuu riskienhallinnan perusta, jonka ympärille voidaan sitten kasata riskienhallinnan muut käytännöt. Toisaalta riskienhallintaprosessi on se ydin, joka tulee liittää niihin yrityksen toimintoihin ja prosesseihin, joihin riskienhallinnan katsotaan luonnollisimmin istuvan. Riskienhallintaprosessi muodostuu toisiaan seuraavista vaiheista: riskien tunnistaminen, analysointi, priorisointi, hallinta ja seuranta. Prosessin vaiheiden menestyk-

sekäs toteuttaminen vaatii lihaa luiden ympärille, joten prosessin kaikkien vaiheiden osalta tulisikin selventää, miten riskienhallinnan työtä kussakin vaiheessa käytännössä tehdään. Esimerkiksi riskien analysoimiseen on olemassa useita erilaisia malleja, joita soveltamalla voidaan päättää, millaisia riskienhallintatoimenpiteitä riskeihin vastaamiseksi tulee tehdä. Riskienhallintaprosessin muodollisella mallintamisella ja sen viestimisellä varmistutaan, että riskienhallinta on jatkuvaa ja systemaattista koko yrityksessä.

Riskienhallintaprosessissa lähtökohtana tulisi olla ne riskit, jotka uhkaavat tavoitteiden saavuttamista. Aineiston analysoinnin yhteydessä todettiin, että yrityksen strategia rakentuu pääasiassa toimialojen strategioista, mikä riskienhallinnan osalta puolestaan tarkoittaa, että koko yrityksen riskit muodostuvat pääasiassa toimialojen riskeistä. POK:ssa onkin koettu haasteelliseksi se, kuinka saadaan muotoiltua riskienhallinta siten, että siinä tartutaan nimenomaan toimialojen riskeihin. Tällä hetkellä yrityksen vuotuisen riskitarkastelun lähtökohta on liiketoiminnassa, mutta riskit eivät silti varsinaisesti polveudu toimialojen riskitarkasteluista, koska sellaisia ei ole olemassa. Toimialojen ”riskianalyysit” muodostuvat SWOT- ja ympäristöanalyyseistä, joiden kysymyksen asettelu ei ole: Mitkä riskit uhkaavat tavoitteiden saavuttamista? Analyyseissä sivutaan riskiä, mutta niissä ei mennä tarpeeksi syvälle, jotta niiden pohjalta voitaisiin kasata koko yrityksen riskikenttä. Tavoitetila siis olisikin, että riskien tunnistaminen ja analysointi tapahtuisi nimenomaan toimialatasolla, josta ne sitten vietäisiin johtoryhmän käsiteltäväksi ja niistä summana muodostuisi yrityksen riskikokonaisuus (kuvio 6). Tietenkin yrityksen tasolla on lisäksi myös muita riskejä, jotka tulee riskienhallinnassa huomioida, mutta pääasiassa riskit kuitenkin syntyvät liiketoiminnasta.



Kuvio 6 Riskitarkasteluiden tavoitetila

Tavoitetilan saavuttaminen edellyttää riskienhallintaprosessin selkiyttämisen ohella myös ohjeistusta, vastuiden määrittelyä, tavoitteiden selkiyttämistä sekä viestintää.

Ohjeistus

Riskienhallintatyötä ohjaamaan kaivataan yrityksessä monentasoista ohjeistusta. Ohjeistusta tarvitaan sekä riskienhallinnan tavoitteiden ja vastuiden selkiyttämiseen että käytännön riskienhallinnan työtä helpottamaan. Riskienhallinnan tavoitteet, vastuut ja raportointiperiaatteet tulisi linjata yrityksen riskienhallintapolitiikassa. Riskienhallinnan tavoitteiden selkeällä määrittelyllä vastataan tarpeeseen selkiyttää koko riskienhallinnan kenttää ja sen tekemisen motiiveja. Riskienhallinnan avulla yrityksessä voidaan ottaa perustellusti suurempia riskejä ja näin saavuttaa liiketoiminnan tavoitteet tehokkaammin ja varmemmin. Riskienhallinnan motiivien ymmärtäminen onkin tärkeää, jotta ohjeistuksen mukaiseen riskienhallintatyöhön sitoudutaan yrityksessä. Jos riskienhallinta koetaan vain turhaksi lisätyöksi, on sen menestyksekäs toteuttaminen vaikeaa. Tavoitteiden ohella vastuiden selkeä osoittaminen on ehdoton edellytys riskienhallinnan onnistumiselle. Tällä hetkellä riskienhallinnan vastuu on jaettu yrityksessä, mutta silti kukaan ei oikein vastaa lopulta mistään. Riskienhallintapolitiikan ohella riskienhallinnan tehtävät pitäisikin liittää työnkuvauksiin, jolloin jokaisella olisi konkreettisesti tiedossa, mikä kuuluu omaan vastuualueeseen, ja näin vältetään turhia päällekkäisyyksiä riskienhallinnan työssä.

Pelkästään kuitenkaan se, että yrityksessä tiedetään, mitä kenenkin pitäisi tehdä, ei riitä. Pitää olla myös työvälineitä ja konkreettisia ohjeita siitä, miten riskienhallintaa tehdään ja miten riskeihin suhtaudutaan. Riskistrategia tulisikin tehdä riskeihin suhtautumisen systematisoimiseksi. Riskistrategiassa tulisi määritellä, millaisia riskejä POK:ssa halutaan hyödyntää, mitä halutaan välttää sekä kuinka paljon riskiä halutaan ottaa. Riskinkantokyvyn ja riskinottohalun määrittelyllä voidaan vastata näistä viimeiseen. Riskinkantokyvyn tulisi yleisesti ohjata riskinottoa yrityksessä. Koska POK:n riskinkantokyky on tällä hetkellä hyvä, eikä riskienhallinnan haluta liikaa jäykistävän yrityksen päätöksentekoa ja muuta toimintaa, voisi riskinkantokyvyn hyödyntäminen tulla kyseeseen vain suurimpien investointien ja hankkeiden osalta.

Riskienhallinnan työvälineiden avulla erityisesti liiketoimintajohdon pitäisi tulevaisuudessa kyetä tehokkaammin ja systemaattisemmin tarkastelemaan liiketoimintaan liittyviä riskejä. Yrityksessä tulisikin luoda vähintäänkin riskianalyysimalleja erilaisia päätöksenteko- ja suunnittelutilanteita varten. Analyysimalleista ei kuitenkaan pitäisi muo-

dostua vain toiminnasta irrallisia tarkistuslistoja, joten riskienhallinta tulisikin liittää yrityksen käytäntöihin ja prosesseihin.

Tasapainotettu mittaristo

Tasapainotettua mittaristoa käytetään POK:ssa johtamisen työkaluna. Siinä asetetaan toiminnalle tavoitteita ja sen avulla seurataan tavoitteiden saavuttamista. Mittaristo toimii siis apuna sekä suunnittelussa että seurannassa. Riskienhallinnan ei haluta olevan muusta toiminnasta irrallinen palanen ja haastatteluissa korostuikin tarve integroida riskienhallinta osaksi yrityksen johtamisjärjestelmää ja toimintoja. Riskienhallinnan liittäminen jo olemassa olevaan johtamisen työvälineeseen onkin vastaus tarpeeseen. Liittämällä riskienhallinta osaksi tasapainotettua mittaristoa, saadaan riskienhallinta luontevasti osaksi toiminnan suunnittelua ja johtamista. Riskejä tulee tarkastella nimenomaan suunnittelun yhteydessä, koska tällöin voidaan tunnistaa, mitkä tapahtumat voivat estää tavoitteiden saavuttamisen ja toisaalta mitä sellaisia mahdollisuuksia voi tulla, jotka edesauttavat tavoitteiden saavuttamisen. Mittaristossa tunnistetut riskit linkitetään mittariston eri näkökulmiin, ja mittareita seuraamalla saadaan tietoa riskienhallinnan keinojen ja käytäntöjen tehokkuudesta.

Liittämällä riskienhallinta tasapainotettuun mittaristoon varmistetaan riskienhallinnan jatkuvuus niin riskien tarkastelun kuin niiden seurannankin osalta. Jatkuvalla seurannalla varmistutaan siitä, että riskienhallintaa on joka hetki ajantasaista ja tehokasta. Riskienhallinnan seuranta ja arviointi puolestaan mahdollistaa riskienhallinnan jatkuvan parantamisen. Lisäksi koska tasapainotettu mittaristo on jo kaikille yrityksessä tuttu on sen hyödyntäminen myös riskienhallinnan sitouttamisen keinona hyvä.

Viestintä

Haastatteluiden perusteella todettiin, että riskienhallinnasta ei raportoida riittävästi ja raportointikäytäntöjä tulisikin selkiyttää POK:ssa. Viestintä onkin kriittinen tekijä niin sitouttamisen kuin riskitietoisuudenkin kannalta. Erityisesti riskienhallintakäytäntöjen muuttaminen edellyttää tehokasta viestintää, jotta yrityksessä tiedetään, miten tulevaisuudessa riskienhallintaa tulee tehdä, kenen sitä tulee tehdä ja miten siitä tulee raportoida. Raportointi on myös riskienhallinnan valvonnan kannalta oleellinen asia. Raportoinnin avulla voidaan varmistua, että riskienhallintaa tehdään yrityksessä kuten on

suunniteltu. Toimialajohdon tulisi raportoida johtoryhmälle ja johtoryhmä puolestaan raportoi hallitukselle. Raportoinnin ohella riskienhallinnan dokumentaation tasoa pitää POK:ssa nostaa. Riskienhallintaprosessin kaikki vaiheet tulee dokumentoida. Dokumentointia varten voidaan kehitellä dokumentointirunko sekä paikka, johon dokumentit tallennettaan. Dokumentoinnin avulla riskienhallinnasta tulee järjestelmällisempää ja lisäksi näin varmistetaan ettei tieto jää yhden ihmisen varaan. Raportointi- ja dokumentointikäytännöistä voidaan viestiä riskienhallintapolitiikan avulla.

5.2 Riskienhallinnan koordinointi tulevaisuudessa

POK:ssa on kaavailtu riskienhallinnan koordinointiin omia resursseja, kontrollerin tehtävänimikkeellä. Koordinoinnilla tarkoitetaan tässä riskienhallinnan työn ohjaamista, työssä avustamista sekä riskienhallinnan seurantaa. Yrityksessä toimii tällä hetkellä kehityspäällikkö, jonka tehtäväkenttään riskienhallinnan koordinointia on myös mietitty. Kokonaan uuden, yrityksen ulkopuolelta tulevan henkilön palkkaaminen nähdään ongelmalliseksi lähinnä siksi, että tällaiselta riskienhallinnan koordinoijalta vaaditaan näkemystä sekä yrityksestä kokonaisuutena että sen erillisistä toimialoista, joilla riskit ovat hyvinkin erilaisia.

Kontrollerin tarve onkin hyvin ajankohtainen, kun riskienhallintaa lähdetään kehittämään. Haastateltavat ovat yhtä mieltä siitä, että riskienhallintaan pitää jatkossa kiinnittää yhä enemmän huomiota ja sen organisoimiseen tarvitaan oma henkilö. Täyttä yksimielisyyttä kontrollerin asemasta organisaatiossa ei kuitenkaan ole. Haastatteluissa nousi esille kaksi erilaista näkökulmaa. Toisen mukaan kontrollerin tulisi olla riippumaton toimija, joka olisi hallituksen alla. Tällöin tehtävät painottuisivat enemmänkin riskienhallinnan seurantaan ja valvontaan. Näin myös toimitusjohtajan työtä voitaisiin valvoa ja arvioida. Toisen näkökulman mukaan kontrolleri toimisi toimitusjohtajan alla ja olisi mukana riskienhallinnan käytännön toteutuksessa ja kehittämisessä.

Yrityksessä tulisi olla taho, joka valvoisi ja arvioisi riskienhallinnan työtä. Tehtävä kuuluu hallitukselle ja hallituksen tahdosta riippuen tällainen lisäresurssi yritykseen jossain vaiheessa mahdollisesti otetaan. Tällä hetkellä POK:n sisäinen tarkastus toimii vain yrityksen operatiivisella tasolla, eikä kykenekään arvioimaan toiminnan strategista puolta.

Aineiston analysoinnin perusteella kontrollerin tulisi kuitenkin tässä vaiheessa riskienhallinnan kypsyyskaarta olla ehdottomasti riskienhallinnan työn kehittämisessä mukana. Riskienhallinnan valvonnan tarve ei tällä hetkellä ole akuutti.

Kontrollerin tehtäväkenttä voisikin muodostua riskienhallinnan asioiden tutkimisesta, niiden esille tuomisesta, riskienhallinnan teknisen toteuttamisen kehittämisestä, riskianalyysien tekemisestä ja riskienhallinnan ohjeistamisesta. Lisäksi kontrollerin tulisi säännöllisesti raportoida johtoryhmälle, missä riskienhallinnan kanssa mennään. Kontrollerista huolimatta liiketoimintajohdolla tulisi olla vastuu riskienhallinnasta, sillä se tuntee parhaiten liiketoimintaan sisältyvät riskit, toimintaympäristön ja kilpailijat. Kontrolleri voisikin olla lähinnä johdon apu ja sparraaja, joka suuntaisi riskienhallintaa oikeaan suuntaan siten, että riskienhallinnalla varmistetaan tavoitteiden saavuttaminen.

6 JOHTOPÄÄTÖKSET

Tutkimuksen tavoitteena oli kehittää case-yrityksen riskienhallintajärjestelmää varten konstruktio, jolla riskienhallinnasta saadaan rakennettua toimivampi ja tehokkaampi kokonaisuus. Tavoitteen saavuttamiseksi tutkimuksessa listattiin riskienhallinnan kriteereitä, jotka riskienhallinnan tulisi täyttää ollakseen toimivaa ja tehokasta sisäisen tarkastuksen näkökulmasta. Lisäksi teoriaosuudessa mallinnettiin riskienhallintajärjestelmä, joka vastaa näihin sisäisen tarkastuksen arviointivaatimuksiin. Sisäisen tarkastuksen kriteerien ja teoreettisen riskienhallintajärjestelmän mallin pohjalta analysoitiin yrityksen riskienhallinnan nykytila sekä esitettiin kehitysehdotukset. Analysointitapa soveltui hyvin tutkimukseen, jossa piti löytää nykyisen järjestelmän heikkoudet ja luoda niiden sekä tutkimuksen haastatteluiden pohjalta suunnitelma, jota kohdeyrityksessä voidaan lähteä kehittämään.

Tutkimuksen tutkimusongelma oli: *Millainen on tehokas riskienhallintajärjestelmä sisäisen tarkastuksen näkökulmasta?* Tähän kysymykseen vastattiin sekä sisäisen tarkastuksen riskienhallinnan kriteereitä listaamalla että teoreettisen riskienhallintajärjestelmän mallintamisella.

Tutkimuksen yhteydessä case-yrityksen toimitusjohtajan ja talousjohtajan kanssa käydyissä keskusteluissa korostui erityisesti tarve kehittää riskienhallinnasta järjestelmä, joka vastaa paremmin liiketoiminnan riskeihin. Tutkimuksessa esitetyt kehityskohteet vastaavat kaikki osaltaan tähän tarpeeseen. Liiketoiminnan tavoitteiden saavuttamista uhkaavien riskien hallitseminen edellyttää, että riskienhallintaa tehdään sillä organisaatiotasolla, jossa riskit syntyvät eli liiketoimintajohdon tulee olla mukana riskityössä. Riskityön tueksi ja sen systematisoimiseksi tarvitaan ohjeistusta siitä, mitä pitää tehdä, kenen pitää tehdä ja miksi pitää tehdä. Viestinnällä varmistetaan, että kaikki osaavat vastata edellä esitettyihin kysymyksiin. Kun riskienhallinnan käytännöt sitten liitetään yrityksen muuhun toimintaa, sen suunnitteluun, päätöksentekoon ja seurantaan, varmistetaan, että riskienhallintaa on jatkuvaa ja ajantasaista.

Haastateltavat esittivät riskienhallintajärjestelmän kehittämisen kannalta kriittiseksi tekijäksi riskienhallintajärjestelmän helppouden ja joustavuuden. Järjestelmän raskaus

koettiinkin sitouttamista vaikeuttavana tekijänä. Tutkimuksessa konstruoidussa mallissa uuden järjestelmän raskaus on pyritty välttämään liittämällä riskienhallinta jo olemassa oleviin järjestelmiin. Malli ei edellytä suuria investointeja tai raskaita järjestelmiä, ja tutkimuksessa korostuukin näiden sijaan työn koordinoinnin ja vastuiden selkiyttämisen merkitys. Toinen tunnistettu kriittinen tekijä oli se ettei riskienhallinnan hyötyjä kyetä näkemään, jolloin riskienhallinta koetaan vain kustannuksia aiheuttavana lisätyönä. Mallissa korostetaankin viestintää, jolla sekä riskitietoutta että riskienhallinnan motiivien ymmärrystä voidaan lisätä. Yrityksessä pitääkin ennen kaikkea ymmärtää riskienhallinnan arvo ja sen hyödyt liiketoiminnan kannalta.

Riskienhallinnan on todettu helposti unohtuvan muiden tärkeämmäksi koettujen asioiden rinnalla ja liiketoiminnan niin sanottu arkinen hoitaminen vie liiketoimintajohdon ajan ja huomion. Tästä johtuen riskienhallinta tulisikin kytkeä liiketoiminnan käytäntöihin ajattelu- ja työskentelytavaksi, mikä mahdollistaa riskienhallinnan tehokkaan toteuttamisen. (Suominen 2003, 31) Riskienhallinnan kehittäminen ja toteuttaminen vaatii usein kuitenkin myös lisäresursseja. Kohdeyrityksessä ollaankin kaavailtu riskienhallinnan työtä koordinoimaan kontrolleria, joka avustaisi uuden riskilähtöisemmän kulttuurin synnyttämisessä. Deloitten määritelmä kiteyttää tämän riskienhallinnan tavoitetilan: *”Riskiälykkäässä organisaatiossa riskienhallintaa ei nähdä projektina vaan osana sen kulttuuria, tapaa tehdä liiketoimintaa”* (Deloitte & Touche LLP 2006, 8).

Tutkimus täytti sille asetetun tavoitteen konstruoimalla kohdeyritykselle suunnitelman riskienhallintajärjestelmästä, jolla riskienhallinnasta saadaan toimivampi ja tehokkaampi kokonaisuus. Malli perustuu pääasiassa haastatteluissa ja tutkimuksen aikana käydyissä keskusteluissa esille tulleisiin ongelmakohtiin. Malli täydentyi vielä tutkimuksen aineiston analyysin yhteydessä. Riskienhallintajärjestelmän kehittäminen on ajallisesti pitkäkestoinen hanke, joten tutkimuksen puitteissa ei ollut mahdollista testata konstruktion toimivuutta käytännössä. Vasta myöhemmin olisi mahdollista tarkastella sitä, kuinka hyvin suunnitelma toimii käytännössä, ja kokeeko yritys tarpeelliseksi viedä suunnitelman kaikki osa-alueet käytäntöön.

Tutkimuksessa havaittiin, että riskienhallintajärjestelmän kehittämisessä on ennen kaikkea kysymys siitä, miten riskienhallinta saadaan luontevasti osaksi organisaation toimintaa sekä kuinka organisaation henkilöstö saadaan ymmärtämään, että riskienhallinta

on normaali osa järkevää liikkeenjohtamista. Riskienhallinnassa ei siis ole kysymys mörköjen maalaamisesta seinille vaan varautumisesta tulevaisuuden epävarmuuksille. Kehittäminen nojaa pitkälti viestintään ja johdon sitoutumiseen sekä riskienhallinnan työhön liittyviin onnistumisiin. Kun huomataan, että riskienhallinnasta todella on hyötyä ja se auttaa tavoitteiden saavuttamisessa, on sitoutuminen riskienhallintaan huomattavasti helpompaa.

Tutkimusten tulokset eivät suoraan ole yleistettävissä muiden organisaatioiden toimintaan. Tapaustutkimukselle onkin tyypillistä ettei tuloksia voida suoraan yleistää tutkimuskohteen ulkopuolelle (Hirsjärvi, Remes & Sajavaara 2004, 134–135). Se ei siis ollut myöskään tutkimuksen tarkoitus. Tutkimuksessa pyrittiin ennen kaikkea kehittämään kohdeyrityksen erityispiirteet huomioiva suunnitelma. Kohdeyrityksen erityispiirteitä ovat muun muassa ketjuohjautuvuus ja usealla toimialalla toimiminen. Kuitenkin analyysitapa, jota tutkimuksessa käytettiin, toimii esimerkkinä siitä, miten riskienhallinnan kehitystarpeita ja -kohteita on mahdollista analysoida. Lisäksi teoriassa esitetty riskienhallintajärjestelmän malli perustuu yleisiin sisäisen tarkastuksen riskienhallinnan arviointikriteereihin, ja näin siinä esitetyt riskienhallintajärjestelmän tekijät ovatkin valideja organisaatiosta riippumatta.

Kokonaisvaltainen riskienhallinta on omaksuttu ajatuksen tasolla sekä useimmissa organisaatiossa että riskienhallinnan kirjallisuudessa (Ai ym. 2012, 29). Kokonaisvaltaisesta riskienhallinnasta onkin tehty paljon tutkimusta ja vielä enemmän on tutkittu perinteistä riskienhallintaa. Kuitenkin vain harva organisaatio todella hallitsee koko riskikirjoaan tehokkaasti kokonaisvaltaisen riskienhallinta-ajattelun mukaisesti (Deloitte & Touche LLP 2006, 2). Samaan aikaan organisaatioiden toimintaympäristö on koko ajan monimutkaisempi ja vaatii yhä parempaa riskeihin varautumista (Räikkönen & Rouhiainen 2003, 3). Tehokkaan riskienhallintajärjestelmän kehittämistä voidaan siis edelleen pitää ajankohtaisena tutkimusaiheena. Aiempaan tutkimukseen verrattuna tutkimus luo lisäarvoa yhdistämällä sisäisen tarkastuksen riskienhallinnan arvioinnin kriteerit riskienhallintajärjestelmän kehittämistä käsittelevään tutkimukseen. Mielenkiintoinen jatkotutkimusaihe olisi tarkastella tutkimuksen teoriaosuudessa esitetyn riskienhallintajärjestelmän mallin yhtä osa-aluetta ja sen merkittävyyttä riskienhallinnan tehokkuuden ja toimivuuden kannalta.

LÄHTEET

Ai J., Brockett P., Cooper W. & Golden L. 2012. Enterprise Risk Management Through Strategic Allocation of Capital. *The Journal of Risk and Insurance,* Vol. 79, No. 1, 29–55.

Alasuutari, P. 1995. *Laadullinen tutkimus.* Tampere: Vastapaino.

Bate, P. 1984. The Impact of Organizational Culture on Approaches to Organizational Problem Solving. *Organization Studies,* Vol. 5, No.1, 43–66.

Blumme N., Karhu P., Kontula L., Laitakari J., Linna M., Nordin J., Sovasto J., Tarvainen J., Tikkanen R., Turakainen O., Urrila A. & Vesa J. 2005. *Corporate Governance sisäisen valvonnan ja riskienhallinnan näkökulmasta.* Helsinki: Edita Publishing Oy.

Branson, B. The Role of the Board of the Directors and Senior Management in Enterrise Risk Management. Teoksessa Fraser, J. & Simkins, B. *Enterprise Risk Management: Today's Leading Research and Best Practices for Tomorrow's Executive.* New Jersey: John Wiley and Sons, 51–68.

Buehler, K., Freeman, A., Hulme R. 2008. Owning the Right Risks. *Harvard Business Review,* September, Vol. 86, Issue 9, 102–110.

Buehler, K. & Pritsch, G. 2003. Running with Risk. *McKinsey Quaterly,* Issue 4, 40–49.

Chapman, C. 2001. The Big Picture. *The Internal Auditor,* June, Vol. 58, Issue 3, 30–37.

Damodaran, A. 2008. *Strategic Risk Taking. A Framework for Risk Management.* New Jersey: Wharton School Publishing.

Deloitte & Touche LLP 2006. *The Risk Intelligent Enterprise: ERM Done Right.*

Drew, S. & Kendrick T. 2005. Risk Management: The Five Pillars of Corporate Governance. *Journal of General Management,* Vol. 31, No. 2, 19–36.

Eriksson, P. & Koistinen, K. 2005. *Monenlainen tapaustutkimus.* Helsinki: Kuluttajatutkimuskeskus.

Eriksson, P. & Kovalainen, A. 2008. Qualitative Methods in Business Research. London: SAGE Publications Ltd.

Eskola, J. & Suoranta, J. 1998. *Johdatus laadulliseen tutkimukseen.* Tampere: Vastapaino.

Fraser, J. & Simkins, B. 2010. *Enterprise Risk Management: Today's Leading Research and Best Practices for Tomorrow's Executive.* New Jersey: John Wiley and Sons.

Frigo, M. & Anderson, R. 2009. Strategic Risk Assessment. A First Step for Improving Risk Management and Governance. *Strategic Finance,* December, 25–33.

Galloway, D. & Funston, R. 2000. The Challenges of Enterprise Risk Management. *Balance Sheet,* Vol. 8, Issue 6, 22–25.

Gibbs, E. & DeLoach, J. 2006. Which Comes First… Managing Risk or Strategy-Setting? Both! *Financial Executive,* Vol. 22, Issue 1, 34–39.

Giddens, A. 1991. *Modernity and Self-Identity. Self and Society in the Late Modern Age.* Cambridge: Polity Press.

Grunig, J. 1992. What is Excellance in Management? Teoksessa Grunig, J. & Grunig, L. (toim.) *Excellance in Public Relations and Communication Management.* New Jersey: Lawrence Erlbaum Associates Inc. Publishers, 219–249.

Gummesson 2000. Qualitative methods in Management Research. Thousand Oaks: SAGE Publications Ltd.

Halla, I., Hätinen, R., Grönfors-Kallio, A., Malm, S, Kaisanlahti, T., Kontula, L. & Väisänen, H. 2003. *Corporate Governance Suomessa.* Helsinki: Edita Publishing Oy.

Head, G. 2009. *Risk Management – Why and How. An Illustrative Introduction to Risk Management for Business Executives.* Dallas: International Risk Management Institute, Inc.

Hirsjärvi, S. & Hurme, H. 2011. *Tutkimushaastattelu. Teemahaastattelun teoria ja käytäntö.* Helsinki: Gaudeamus.

Hirsjärvi, Remes & Sajavaara 2009. *Tutki ja kirjoita*. Helsinki: Tammi.

Holopainen A., Koivu E., Kuuluvainen A., Lappalainen K., Leppiniemi J., Mikola M. & Vehmas K. 2006. *Sisäinen tarkastus.* Helsinki: Tietosanoma Oy.

Hoyt, R. & Liebenberg, A. 2011. The Value of Enterprise Risk Management. *The Jour nal of Risk and Insurance,* Vol. 78, No. 4, 795–822.

Ingley, C. & Van Der Walt, N. 2008. Risk Management and Board Effectiveness. *International Studies of Management & Organization,* Vol. 38, No. 3, 43–70.

Jorgensen, J. 2011 What Happened to ERM? *Internal Auditor,* Vol. 68, Issue 4, 63–65.

Kaplan, R. & Norton, D. 2006. *Alignment Using the Balanced Scorecard to Create Corporate Synergies.* Boston: Harvard Business School Press.

Kaplan, R. & Norton, D. 2004. *Strategiakartat, aineettoman pääoman muuttaminen mitattaviksi tuloksiksi.* Helsinki: Talentum Media Oy.

Kaplan, R. & Norton, D. 2002. *Strategialähtöinen organisaatio. Tehokkaan strategia-prosessin toteutus.* Helsinki: Talentum Media Oy.

Kaplan, R. & Norton, D. 1996. *The Balanced Scorecard.: Translating strategy into Action.* Boston: Harvard Business School Press.

Kasanen, E., Lukka, K. & Siitonen, A. 1993. The Constructive Approach in Management Accounting Research. *Journal of Management Accounting Research,* Vol. 5, 243–264.

Kauppinen, T. 2002. *Arvojohtaminen.* Helsinki: Kustannusosakeyhtiö Otava.

Kihn, L. & Näsi, S. 2011. Tilintarkastusta käsittelevien väitöskirjojen tutkimus-strategiset valinnat – Aihepiiri ja tutkimusote. In: Contributions to Accounting, Auditing and Internal Control. Essays in Honour of Professor Teija Laitinen. Acta Wasaensia No. 234, 61–87. Eds Annukka Jokipii & Johanna Miettinen.

Kimbrough L. & Componation P. 2009. The Relationship Between Organizational Culture and Enterprise Risk Management. *Engineering Management Journal,* June, Vol.21, No. 2, 18–26.

Kimbrough, L. & Componation, P. 2005. The Best Fit. *The Internal Auditor,* April, Vol. 62, Issue 2, 48–49.

Koskinen, I., Alasuutari, P. & Peltonen, T. 2005. *Laadulliset menetelmät kauppatieteissä.* Jyväskylä: Vastapaino.

KPMG 2005. *Corporate Governance sisäisen valvonnan ja riskienhallinnan näkökulmasta.* Helsinki: Edita Publishing Oy.

Kupi E., Keränen J., Lanne M. 2009. *Riskienhallinta osana pk-yritysten strategista johtamista.* VTT. Working Papers 137.

Kyrölä, T. 2010. *Liiketoiminnan strateginen johtaminen: Strategiset päätökset jatkuvuudenhallinnan johtamiseksi.* Aalto-Yliopiston kauppakorkeakoulu: B-121.

Laamanen, K. 2005. *Johda liiketoimintaa prosessien verkkona: ideasta käytäntöön*. 6. painos. Keuruu: Otava.

Lam, J. 2003. *Enterprise Risk Management: From Incentives to Controls.* John Wiley & Sons Inc.

Leech, T. 2000. The Next Wave in Assurance Thinking. *The Internal Auditor,* Vol. 57, Issue 4, 66.

Leino, M., Steiner, M-L. & Wahlroos, J. 2005. Corporate Governance ja riskienhallinta. Teoksessa Kuusela, H. & Ollikainen, R. (toim.) *Riskit ja riskienhallinta.* Tampere: Tampereen yliopistopaino Oy - Juvenes Print, 123–147.

Lindow, P. & Race J. 2002. Beyond Traditional audit Techniques. *Journal of Accountancy,* July, Vol. 194, Issue 1, 28–33.

Malmi, T., Peltola, J. & Toivanen, J. 2006. *Balanced Scorecard*. Helsinki: Talentum.

Marques, J. 2010. Enhancing the Quality of Organizational Communication, A Presentation of Reflection-based Criteria. *Journal of Communication Management,* Vol. 14, No. 1, 47–58.

McShane, M., Nair, A. & Rustambekov, E. 2011. Does Enterprise Risk Management Increase Firm Value? *Journal of Accounting, Auditing & Finance,* Vol. 26, No. 4, 641-658.

Nottingham, L. 1997. *A Conceptual Framework for Integrated Risk Management.* Members' Briefing Publication 212-97, The Conference Board of Canada, September.

Pettigrew, A. 1979. On Studying Organizational Cultures. *Administrative Science Quaterly,* Vol. 24, No. 4*4,* 570–581.

Pickett, K. 2005. *Auditing the Risk Management Process.* New Jersey: John Wiley & Sons, Inc.

Psica, A. 2007. Destination Ahead. *Internal Auditor,* February, Vol. 64, Issue 1, 77–80.

PwC 2008. *A Practical Guide to Risk Assessment: How Principles-based Risk Assessment Enables Organizations to Take the Right Risks.*

Rappaport, A. 1998. *Creating Shareholder Value. A Guide for Managers and Investors.* New York: The Free Press.

Raz, T. & Hillson, D. 2005. A Comparative Review of Risk Management Standards. *Risk Management: An International Journal,* Vol. 7, No. 4, 53–66.

Reigle, R. 2001. Measuring Organic and Mechanistic Cultures. *Engineering Management Journal,* Vol. 13, No. 4, 3–8.

Rosa, S. 2007. Moving forward with ERM. *The Internal Auditor,* June, Vol. 64, Issue 3, 50–54.

Räikkönen, T. & Rouhiainen, V. 2003. *Riskienhallinnan muutosvoimat. Kirjallisuuskatsaus.* VTT Tiedotteita 2208. Espoo: VTT, Valtion teknillinen tutkimuskeskus.

Schein, E. 1987. *Organisaatiokulttuuri ja johtaminen.* Espoo: Weilin+Göös.

Schild, P. 2009. Improving Risk Management: Process and Culture. *Financial Execu-*

tive, Vol. 25, Issue 4, 55.

Shenkir, W. & Walker, P. 2011. *Enterprise Risk Management: Frameworks, Elements, and Integration.* New Jersey: Institute of Management Accountants.

Shenkir, W. & Walker, P. 2007. *Enterprise Risk Management: Tools and Techniques for Effective Implementation.* New Jersey: Institute of Management Accountants.

Shortreed, J. 2010. Enterprise Risk Management and ISO 31000. *The Journal of Policy Engagement,* June, Vol. 2, No. 3, 8–10.

Skurnik, S. 2002. Osuustoiminnan merkitys. Avausluku Seppo Pöyhösen kirjassa *Osuuskunnan hallinto ja osuuskuntalaki.* Jyväskylä: Gummerus, 1–15.

Sobel P. & Kapoor G. 2012. Step Up to the Plate. *The Internal Auditor,* April, Vol. 69, Issue 2, 41–44.

Stirling, A. 1998. Risk at a turning point? *Journal of Risk Research*, Vol. 1, Issue 2, 97-109.

Suominen, A. 2005. Kokonaisvaltainen riskienhallinta yrityksen suojausjärjestelmänä. Teoksessa Kuusela, H. & Ollikainen, R. (toim.) *Riskit ja riskienhallinta.* Tampere: Tampereen yliopistopaino Oy - Juvenes Print, 148–169.

Suominen, A. 2003. *Riskienhallinta.* Helsinki: Werner Söderström Osakeyhtiö.

Tuomi J. & Sarajärvi A. 2009. *Laadullinen tutkimus ja sisällönanalyysi.* Helsinki: Tammi

Veijola, R. 2012. ISO 31000 -standardi – riskienhallinta tulee osaksi organisaation kaikkea toimintaa. *Tilintarkastus,* 4/2012.

Viitala, R. 2004. *Henkilöstöjohtaminen.* Helsinki: Edita.

Virolainen, H. 2010. *”Kai sitä ihminen on vaan semmoinen laumaeläin” – Virtuaalisen tiimin ilmapiiri.* Turun kauppakorkeakoulu: Sarja A-8:2010.

Vos, M. & Schoemaker, H. 2005. *Integrated Communication. Concern, Internal and Marketing Communication.* Utrecht: Lemma Publishers.

Wood, P. 2005. Risk Management Off the Shelf and into Practice. *Manager: British Journal of Administrative Management*, Feb/Mar 2005, Issue 45, 26–27.

Standardit, suositukset, raportit ja viitekehykset

AIRMIC, ALARM & IRM 2010. *A Structured Approach to Enterprise Risk Management (ERM) and the Requirements of ISO 31000.*

AIRMIC, ALARM & IRM 2002. *A Risk Management Standard.* <http://www.theirm.org/publications/documents/Risk_Management_Standard_030820.pdf.> 30.8.2012

AS/NZC 4360:2004. *Australian/New Zealand Standard Risk Management.* Standards Australia/Standards New Zealand.

AS/NZC ISO 31000:2009. *Risk Management – Principles and Guidelines*. Standards Australia/Standards New Zealand.

Finanssivalvonta, standardi 4.1 Sisäisen valvonnan järjestäminen. Antopäivä 27.5.2003.

International Organization for Standardization, ISO 2009. *Risk Management – Principles and Guidelines.* ISO 31000:2009.

International Organization for Standardization, ISO 17799 standardi. Saatavilla osoitteesta: <http://www.iso.org/iso/catalogue_detail?csnumber=39612>

Sisäiset tarkastajat ry 2010. *Sisäisen tarkastuksen kansainväliset ammattistandardit - International Standards for the Professional Practice of Internal Auditing*. Standardien käännös 10.12.2010. The Institute of Internal Auditors.

The Committee of Sponsoring Organizations of the Treadway Commission, COSO 2004. *Enterprise Risk Management – integrated Framework. Executive Summary Framework.*

The Institute of Internal Auditors (IIA) 2010. *Assessing* the *Adequacy of Risk Management Using ISO 31000.* IPPF - Practice Guide.

The Institute of Internal Auditors (IIA) 2009. *The Role of Internal Auditing in Enterprise-wide Risk Management.* IIA Position Paper.

WWW-sivut

AON 2007. *Enterprise Risk Management: The Full Picture.* <http://secure.eloqua.com/web/AON/Enterprise%20Risk%20Management%20-%20The%20full%20picture_0.pdf?elq_mid=&elq_cid=3012454 > 13.9.2012

Cooper, Speh & Downey 2012. *Creating a Culture of Risk Management*. A Position Paper. <http://www.aba.com/Members/Offers/Documents/e77252939398440490356 75146cc82adWoltersKluwer_Creating_a_Culture_of_Risk_Managemen.pdf>

The Economist Intelligence Unit 2007. *Best practice in risk management. A function comes of age.* <http://www.managementthinking.eiu.com/sites/default/files/eiu_Risk_Management.pdf> 1.9.2012

Holmquist, E. 2011. *The Evolving Role of the Chief Risk Officer.* <*http://ermadvantage.com/2011/11/01/evolving-role-of-the-cro/*> 2.1.2013

ISACA <http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx> 23.08.2012

Layton, M. & Fuchs, M. 2007. *Risk Management Practices Cannot Be "Bolted On".* <http://www.irmi.com/expert/articles/2007/deloitte07.aspx> 19.9.2012

Malmén, Y. & Wessberg, N. 2011. VTT Tuotteet ja tuotanto. *Mitä tarkoitetaan riskillä, riskianalyysillä, riskin arvioinnilla ja riskienhallinnalla?* <http://www.nbcsec.fi/spt/artikkeleita/art-01.pdf> 1.10.2012

Miccolis, J. 2003. *ERM Lessons Across Industries.* IRMI.com, Expert Commentary. <http://www.irmi.com/expert/articles/2003/miccolis03.aspx> 11.9.2012

Pirkanmaan Osuuskaupan vuosikertomus 2011. <http://www.digipaper.fi/pirkanmaan_osuuskauppa/89576/index.php?pgnumb=9> 10.2.2013

Raynor, M. 2007. *Intersection of Strategic Planning and Risk Management.* <http://www.poole.ncsu.edu/erm/index.php/articles/entry/michael-raynor-roundtable/> 17.9.2012

Roche, D. 2012. *Embedding Risk Culture.* <http://www.cso.com.au/article/416830/embedding_risk_culture/> 14.9.2012

S-kanava: ketjut ja palvelut. <http://www.s-kanava.fi/web/s/s-ryhma/ketjut-ja-palvelut> 10.2.2013

S-kanava: osuuskaupat. <http://www.s-kanava.fi/web/s/s-ryhma/osuuskaupat> 10.2.2013

S-kanava: omistusrakenne. <http://www.s-kanava.fi/web/s/s-ryhma/omistusrakenne> 10.2.2013

S-kanava: yritysprofiili. <http://www.s-kanava.fi/web/s/s-ryhma/yritysprofiili> 10.2.2013

S-kanava, Pirkanmaa: hallinto ja johto. <http://www.s-kanava.fi/web/pirkanmaa/hallinto-ja-johto> 10.2.2013

Haastattelut

Kaikko Jukka, kaupallinen johtaja, Pirkanmaan Osuuskauppa, 21.9.2012. Kesto 50 minuuttia.

Koskenniemi Anna, riskienhallintapäällikkö, SOK, 12.7.2012. Kesto 55 minuuttia.

Koskinen Mikko, riskienhallinnan päällikkö, SOK, 29.6.2012. Kesto 55 minuuttia.

Mäki-Ullakko Timo, toimitusjohtaja, Pirkanmaan Osuuskauppa, 24.9.2012. Kesto 90 minuuttia.

Päivinen Anu, toimialajohtaja ABC- ja ravintolakauppa, 21.9.2012. Kesto 50 minuuttia.

Rämö Sari, hallituksen jäsen, Pirkanmaan Osuuskauppa, 27.9.2012. Kesto 50 minuuttia.

Toikkonen Mikko, hallituksen jäsen, Pirkanmaan Osuuskauppa, 27.9.2012. Kesto 50 minuuttia.

Uusi-Seppä Jouni, talousjohtaja, Pirkanmaan Osuuskauppa, 26.9.2012. Kesto 50 minuuttia.

LIITTEET

LIITE 1: Haastattelukysymykset johdolle ja hallitukselle

Yleisesti riskeistä

1. Miten määrittelet sanan riski?

2. Miten saat tietoa riskeistä?

3. Kuinka tärkeää riskitieto on työssäsi?

Yleisesti riskienhallinnasta

4. Mitkä ovat riskienhallinnan motivaatiotekijät eli miksi sitä tehdään?

5. Koetteko, että riskienhallinnan tarpeelliseksi? Miksi?

6. Millaista riskienhallintanne on luonteeltaan?

7. Onko yrityksessänne olemassa keinoja, joilla varmistutaan, että riskinottaminen on järkevää?

Riskienhallintaprosessi

8. Käytättekö jotakin yleistä riskienhallinnan mallia/viitekehystä riskityön ohjaamiseen?

9. Mistä riskienhallinnassa lähdetään liikkeelle?

10. Voisitko kuvailla riskienhallintaprosessianne vaihe vaiheelta?

Riskienhallinnan ohjeistus

13. Onko olemassa riskienhallintapolitiikkaa tai vastaavaa dokumenttia, joka ilmaisee johdon tahtotilan riskienhallinnan suhteen? Mitä se käsittää?

14. Onko olemassa muuta ohjeistusta riskienhallinnasta?

15. Onko yrityksessänne määritelty riskinkantokyky? Ohjaako se riskinottoa?

16. Miten ohjeistus on viestitty yrityksessä?

Riskitietoisuus ja kommunikointi

17. Miten riskienhallinnasta raportoidaan?

18. Mitä riskienhallinnasta dokumentoidaan?

19. Millaista kommunikointia teillä on riskeihin liittyen?

20. Onko kommunikointi mielestäsi riittävää?

Roolit ja vastuut

21. Miten riskienhallinta on organisoitu tällä hetkellä? Kuka tekee ja mitä tekee?

22. Miten riskienhallinta tulisi mielestänne organisoida tulevaisuudessa?

23. Onko olemassa selkeä ohjeistus siitä, kenen vastuulle riskienhallinta kuuluu?

24. Kuka on lopullisessa vastuussa riskienhallinnasta?

Organisaatiokulttuuri

25. Millainen organisaatiokulttuuri yrityksessänne mielestänne on?

26. Onko organisaatiokulttuurilla mielestänne vaikutusta riskienhallintaan?

Strategia ja toiminnan ohjaus

27. Millainen yrityksenne strategiaprosessi on?

28. Huomioidaanko riskit strategiaprosessissa?

29. Millaisia toiminnan ohjausjärjestelmiä teillä on?

30. Voisiko riskienhallinnan liittää olemassa oleviin toiminnan ohjausjärjestelmiin?

Päätöksenteko

31. Huomioidaanko riskit päätöksenteossa?

Prosessit

32. Onko riskit huomioitu prosesseissa?

Riskienhallinnan kypsyysarvioinnit

33. Seuraavassa on kirjallisuudesta poimittu riskienhallinnan kypsyyttä kuvaava jaottelu. Missä arvioisitte riskienhallintanne osalta olevan?

1. Tilapäinen apu: Riskienhallinta on kaoottista ja epävakaata. Ei ole dokumentoitu mitään riskienhallintaan liittyvää ja riskienhallinta on kontrolloimatonta ja riskeihin reagoidaan vain tarpeen tullen.

2. Alustava malli: Riski määritellään eri tavoin organisaatiossa ja riskejä johdetaan toisistaan erillään. Riskienhallinnan prosessi ei ole täsmällinen.

3. Riskienhallinta on määritelty: Yleinen viitekehys riskien tunnistamiseen ja niiden hallintaan on olemassa. Riskienhallintaan ryhdytään merkittävimpien riskien välttämiseksi.

4. Integroitu: Riskienhallintaa toteutetaan kaikilla liiketoiminta-alueilla. Riskejä valvotaan ja mitataan sekä niistä raportoidaan koko yrityksessä. Riskeihin liittyen tehdään skenaarioanalyysia ja riskienhallinnan toimivuutta arvioidaan.

5. Optimoitu: Riskienhallinta on osa strategista suunnittelua ja päätöksentekoa. Riskienhallinnan fokus on jatkuvassa parantamisessa ja muutoksia tehdään tarpeen mukaan.

Riskienhallinnan kehittäminen

34. Miten riskienhallintaa tulisi mielestänne kehittää lähivuosina?

35. Mikä on riskienhallinnan tavoitetila?

36. Mitkä ovat merkittävimmät syyt sille, että riskienhallintaa halutaan kehittää?

37. Mitkä koette suurimmiksi esteiksi riskienhallinnan tehokkaalle ja toimivalle järjestämiselle?

Riskienhallinnan arviointi

38. Arvioidaanko teillä riskienhallinnan toimivuutta ja tehokkuutta? Jos niin miten?

Seuraavat kysymykset esitetty vain hallituksen jäsenille:

Kuinka usein ja mitä teille raportoidaan yrityksen riskeistä ja riskienhallinnasta?

Millä tavalla hallitus käsittelee riskejä ja riskienhallintaa?

Koetteko tarvitsevanne apua riskienhallinnan arviointitehtävässä?

LIITE 2: Haastattelukysymykset riskienhallintapäälliköille

SOK-näkökulma

1. Miten määrittelette riskin?

2. Millainen on SOK:n riskienhallintaprosessi?

3. Mitkä olette kokeneet kokonaisvaltaisen riskienhallinnan suurimmiksi hyödyiksi?

4. Miten SOK määrittelee riskinkantokyvyn ja riskinottohalun?

Osuuskauppanäkökulma

5. Millä tavalla riskienhallinta tulisi mielestänne osuuskaupoissa järjestää?

6. Millaisia työvälineitä SOK on antanut osuuskaupoille riskienhallintatyöhön?

7. Mitä mieltä olette riskienhallinnan liittämisestä tuloskortteihin?

8. Pitäisikö riskienhallinnan työtä ohjaamaan olla osuuskaupoissa kontrolleri tai vastaava henkilö?

9. Mikä sisäisen tarkastuksen rooli tulisi olla riskienhallinnassa?

10. Miten riskienhallintaa tulisi arvioida osuuskaupoissa?

11. Mitkä ovat riskienhallinnan tärkeimmät kehityskohteet osuuskaupoissa?

12. Osuuskauppojen riskienhallintaan on suunniteltu kypsyysarviointeja. Mitä tämä tarkoittaa käytännössä?